



Cybercrime

Bundeslagebild 2020

Inhaltsverzeichnis

Hinweis:

Aus Gründen der besseren Lesbarkeit wird in diesem Lagebild
das generische Maskulinum verwendet.

1 Cybercrime 2020



Die Anzahl erfasster Cyberstraftaten steigt weiter an.



Der Fokus von Cyberkriminellen liegt vermehrt im Bereich „Big Game Hunting".



Die Täter sind global vernetzt und agieren zunehmend professioneller.



Ransomware bleibt weiterhin die Bedrohung für öffentliche Einrichtungen und Wirtschaftsunternehmen.



Die Anzahl an DDoS-Angriffen steigt weiter an – auch ihre Intensität nimmt zu.



Die Underground Economy wächst – sie stellt eine kriminelle, globale Parallelwirtschaft dar, die maßgeblich auf finanziellen Profit aus ist.

Abbildung 1: Die wesentlichen Aspekte der Cybercrime in Deutschland 2020

Cybercrime und Corona: Die Einflüsse der Pandemie



Homeoffice & Social Distancing

Die Gesellschaft greift im Zuge der Corona-Maßnahmen vermehrt auf digitale Angebote zurück. Streaming-Dienste, Messenger-Dienste und Online-Shops verzeichnen einen starken Anstieg ihrer Nutzerzahlen.

Für Cyberkriminelle geht damit eine erhöhte Bandbreite an Tatgelegenheiten einher. Sie verwenden die Corona-Pandemie als Narrativ ihrer Angriffe und wenden diese auf altbekannte Modi Operandi an.

Primäre Bedrohungen



Phishing-Seiten und -Mails, welche sensible Daten abgreifen.

Massive Malspam-Kampagnen, welche Malware-Familien distribuieren.

DDoS-Angriffe, die digitale Lehrplattformen oder VPN-Server lahmlegen können.

Ransomware-Angriffe auf öffentliche Einrichtungen, vor allem das Gesundheitswesen.



Corona-Bekämpfung / Impfstoff-Distribution

Seit Q3 2020:
Vermehrte Angriffe auf Unternehmen und öffentliche Einrichtungen, welche bei der Bekämpfung der Corona-Pandemie relevant sind.

Die Impfstoffherstellung / -distribution und die damit gestiegene Relevanz ganzer Lieferketten erhöhen die Kritikalität von Cyberangriffen in diesem Bereich.

Lessons Learned

1. **Cyberkriminelle passen sich schnell gesellschaftlichen Notlagen an** und nutzen diese gekonnt für ihre Zwecke aus. Sie greifen Institutionen und Unternehmen mit gesellschaftlich hohem Stellenwert, aber auch Privatpersonen an.
2. Die Krise zeigt: **Eine erhöhte Cyber-Security-Awareness** ist beim **Schutz von IT-Infrastrukturen und Unternehmensnetzwerken essentiell.** Sie sollte daher in jedem Unternehmen gefördert werden.
3. **Das Gefährdungspotenzial, welches von Cyberangriffen ausgeht, ist weiterhin auf einem hohen Niveau.** Angriffe auf Akteure, die für die Krisenbewältigung relevant sind, finden infolge ihrer Bedeutung für Politik, Gesellschaft und Wirtschaft vermehrt statt.
4. Um schnell auf dynamische Veränderungen im Bereich der Cybercrime reagieren und strafprozessuale Maßnahmen einleiten zu können, muss eine **stetige Lageevaluierung** erfolgen. **Kooperationen zwischen Polizeibehörden und privaten Institutionen** sind hierfür im Bereich Cybercrime **von besonderer Bedeutung**.

Abbildung 2: Wesentliche Aspekte der Cybercrime während der Corona-Pandemie 2020

Cybercrime Timeline 2020

Januar

Am 07.01.20 unterlagen Server eines IT-Finanz-Dienstleisters einem DDoS-Angriff mit der Folge, dass unter anderem die Webseite und die Online-Banking-Möglichkeiten einer bekannten Bank ausfielen. Kunden konnten sich nicht in ihre Konten einloggen, Überweisungen tätigen oder Daueraufträge anlegen.

Februar

Am 15.02.20 wurde ein Automobilzulieferer, der unter anderem Turbolader für Audi, BMW, VW und Ferrari herstellt, Opfer eines Ransomwareangriffes. Sowohl Standorte in Deutschland als auch im europäischen Ausland waren betroffen. Die Ransomware "Cl0p" verschlüsselte 130 Server und 600 Clients – und auch die Backups.

März

Am 29.03.20 stellte ein international tätiger Pharmakonzern einen Angriff mittels einer Ransomware fest. Weite Teile des weltweiten Firmennetzwerks inklusive vieler Server und Backupserver wurden verschlüsselt. Die als Datei aufgefundene Täter-Forderung deutete auf die Ransomware "Prolock" hin.

April

Die Verantwortlichen eines kommunalen Versorgungsunternehmens mit Sitz in Ludwigshafen stellten am 20.04.20 fest, dass sie Opfer eines Hackerangriffes geworden sind. Die von den Tätern beabsichtigte Verschlüsselung der Systeme mittels der Ransomware "Cl0p" scheiterte zwar, allerdings konnte ein Abfluss von Daten, die später dann im Darknet veröffentlicht wurden, nicht verhindert werden.

Mai

Im Mai wurde bekannt, dass Hacker mehrere Forschungszentren in Europa angegriffen haben, wodurch einige sog. Supercomputer in Deutschland kompromittiert wurden. Eintrittsvektor waren zuvor ausgelesene Nutzerdaten, worüber eine Backdoor installiert werden konnte. Es bestanden Verdachtsmomente, dass weitere Daten abgeflossen sind und die Rechner für das Kryptomining genutzt wurden.

Juni

Über einen bösartigen E-Mail-Anhang wurden am 11.06.20 weite Teile der IT einer mittelständischen Unternehmensgruppe mit Sitz in Süddeutschland, welche unter anderem im Handel mit Baumaschinen tätig ist und allein in Deutschland über 38 Niederlassungen verfügt, verschlüsselt. Für die Entschlüsselung forderten die Täter ein Lösegeld im siebenstelligen Eurobereich – zahlbar in Bitcoin.

Abbildung 3: Zeitliche Auflistung relevanter Cyberangriffe in Deutschland 2020 – Teil 1

Juli	Ein börsennotiertes Unternehmen, welches u. a. im Bereich der Halbleiterherstellung tätig ist, wurde Anfang Juli Opfer der Ransomware "MAZE". Folge: Die IT-Infrastruktur des Unternehmens wurde verschlüsselt und die Täter drohten bei Nichtzahlung der geforderten Summe mit der Veröffentlichung von Kundendaten. Allein am Standort in Deutschland waren 750 Mitarbeitende durch den Angriff nicht mehr arbeitsfähig.
August	Die Gruppierung "Fancy Bear" machte mit einem DDoS-Angriff bei einem deutschen Finanzinstitut auf sich aufmerksam und flankierte die Drohung weiterer Angriffe mit einer Erpressungsmail. Bereits in den Jahren 2017 und 2019 konnten gleichgelagerte Fälle mutmaßlich dieser Gruppierung in Deutschland festgestellt werden.
September	Ein Universitätsklinikum in NRW wurde Mitte September Opfer eines Ransomware-Angriffs. Durch den Angriff wurden 30 Server verschlüsselt und die Klinik-IT lahmgelegt. Akute Fälle konnten nicht mehr aufgenommen und mussten auf umliegende Krankenhäuser verteilt werden.
Oktober	Am 09.10.20 stellte eines der größten deutschen Unternehmen der Computerspielbranche mit Hauptsitz in Frankfurt/M. fest, dass seine gesamte interne Windows-Infrastruktur verschlüsselt wurde. Lösegeldforderungen fanden sich nicht nur als Datei auf Servern und Arbeitsplatzrechnern, sondern auch als Ausdruck in jedem Drucker. Aufgrund der Lösegeldforderung konnte auf die Ransomware "Egregor" geschlossen werden. Die Erpresser gaben an, nicht nur Daten verschlüsselt, sondern auch kopiert zu haben. Mit einer schrittweisen Veröffentlichung von internen Daten wurde gedroht, was im weiteren Verlauf auch erfolgte.
November	Eine Landesrundfunkanstalt wurde am 07.11.20 Opfer einer DDoS-Attacke. Der Angriff führte zum zeitweisen Ausfall der Webseite, sodass keine neuen redaktionellen Beiträge veröffentlicht und keine digitalen Angebote aktualisiert werden konnten.
Dezember	Am 12.12.20 wurde bei einem börsennotierten Unternehmen der Lebensmittel- und Kosmetikbranche ein Angriff auf deren weltweite IT-Infrastruktur festgestellt. Große Teile der Systeme wurden verschlüsselt, sodass ein Produktions- und Kommunikationsausfall nicht verhindert werden konnte. Der dabei entstandene wirtschaftliche Schaden wurde auf mehrere Millionen Euro pro Ausfalltag geschätzt. Über ein schadhaftes Excel-Dokument wurde weitere Schadsoftware wie ein Remote-Access-Trojaner (RAT) und die „Cl0p“-Ransomware nachgeladen und ausgeführt.

Abbildung 4: Zeitliche Auflistung relevanter Cyberangriffe in Deutschland 2020 – Teil 2

Herausragende polizeiliche Maßnahmen

Takedown des EMOTET-Botnetzes und Festnahme eines Verantwortlichen.

(01/2021 – Meldung BKA)

Abschaltung des Darknet-Marktplatzes "DarkMarket".

Festnahme des Webseiten-Betreibers.

(01/2021 – Meldung LKA NI)

Festnahme von zwei Cybertätern im Zusammenhang mit DDoS-Angriffen auf Unternehmen aus dem Finanzsektor.

(06/2020 -Meldung LKA SH - BKA)

Schließung von illegalen Marktplätzen auf Telegram.

Durchführung von bundesweiten Exekutivmaßnahmen.

(10/2020 – Meldung BKA)

Länderübergreifende Maßnahmen gegen Betreiber und Mitglieder des Online-Forums "crimenetwork.co".

(06/2020 – Meldung LKA BB)

Identifizierung von drei Cybertätern und Vollstreckung von Durchsuchungsbeschlüssen im Zusammenhang mit fortlaufenden Brute-Force-Attacken auf ein Eisenbahninfrastrukturunternehmen

(09/2020 – Meldung LKA HE)

Abbildung 5: Herausragende polizeiliche Maßnahmen in Deutschland 2020

2 Allgemeine Informationen

Das Bundeslagebild Cybercrime 2020 wird durch das Bundeskriminalamt in Erfüllung seiner Zentralstellenfunktion erstellt. Es enthält die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cybercrime in Deutschland und bildet die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungsaktivitäten ab.

Schwerpunkt des Bundeslagebild Cybercrime sind die Delikte, die sich z. B. gegen das Internet und informationstechnische Systeme richten – die sog. Cybercrime im engeren Sinne (CCieS).[1] Die einzelnen Delikte dieses Phänomenbereichs werden unter Punkt 8.1 genauer beschrieben.

Das Tatmittel Internet gewinnt im Zuge fortschreitender Digitalisierung in fast allen Deliktsbereichen zunehmend an Bedeutung. Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und nicht der CCieS zugeordnet werden können, bleiben bei den Betrachtungen in diesem Bundeslagebild weitestgehend außen vor.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Hier wird das sog. Hellfeld abgebildet, also die polizeilich bekannt gewordene Kriminalität. Valide Aussagen und Einschätzungen zu Art und Umfang des komplementären Dunkelfeldes, also den Straftaten, die der Polizei nicht bekannt werden, können aus den statistischen Grunddaten der PKS nicht abgeleitet werden. Wie im nachfolgenden Punkt beschrieben, ist im Bereich Cybercrime das Dunkelfeld weit überdurchschnittlich ausgeprägt, so dass es für eine zutreffende Lagebeschreibung von Bedeutung ist, die qualitative Aussagekraft des polizeilichen Hellfeldes zu erhöhen, indem verstärkt auch polizeiexterne Erkenntnisse in die Lagebilderstellung einbezogen werden.

Zu diesem Zweck flossen in das Bundeslagebild Cybercrime 2020 auch Erkenntnisse und Einschätzungen anderer Behörden sowie ausgewählter privatwirtschaftlicher oder wissenschaftlicher Einrichtungen und Verbände ein.

[1] Definitionen zu CCieS, CCiwS etc. s. Appendix S. 42

3 Die Polizeiliche Kriminalstatistik

3.1 HELLFELD VS. DUNKELFELD

Das BKA erstellt die PKS für die Bundesrepublik Deutschland auf der Grundlage der von den Polizeien der Länder und des Bundes gelieferten Daten. Die PKS enthält die der Polizei bekannt gewordenen Straftaten einschließlich der mit Strafe bedrohten Versuche und weitere Angaben zu den registrierten Fällen.

Die bekannt gewordenen Straftaten werden erst nach Abschluss der polizeilichen Ermittlungen erfasst. Die PKS ist damit eine Ausgangsstatistik, die lediglich das polizeiliche Hellfeld abbildet. Im Bereich Cybercrime ist aus nachfolgend aufgeführten Gründen das zugehörige Dunkelfeld weit überdurchschnittlichen ausgeprägt:

- Eine große Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen meist nicht über das Versuchsstadium hinaus und wird von den Geschädigten nicht bemerkt.

- Die Opfer erkennen ihre Betroffenheit nicht (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop). Die von ihnen eingesetzten technischen Geräte werden unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht (z. B. bei Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen).

- Straftaten werden durch die Betroffenen oftmals nicht angezeigt, insbesondere dann, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z. B. Versicherung) reguliert wird.

- Geschädigte, insbesondere Wirtschaftsunternehmen, zeigen erkannte Straftaten nicht an, um u. a. die Reputation als „sicherer und zuverlässiger Partner" im Kundenkreis nicht zu verlieren.

- Geschädigte erstatten oftmals, z. B. in Erpressungsfällen, nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.

3.2 GESAMTSTATISTIK ZU CYBERCRIME IM ENGEREN SINNE

Die Anzahl der in der PKS registrierten Straftaten im Bereich Cybercrime ist in den vergangenen Jahren kontinuierlich angestiegen. Insgesamt hat das Bundeskriminalamt für 2020 rund 108.000 Delikte der Cybercrime im engeren Sinne registriert, was eine erneute Steigerung von +7,9 % im Vergleich zu den 2019 erfassten Fällen bedeutet.

Der stetige Anstieg des Fallaufkommens kann insbesondere auf folgende Aspekte zurückgeführt werden:

- Stark voranschreitende Digitalisierung aller Lebensbereiche, die coronabedingt einen zusätzlichen Antrieb erhielt – dadurch entstehen mehr Tatgelegenheiten für Cyberkriminelle.
- Zunehmende Professionalisierung der Täter und steigende Fähigkeiten der Schadsoftware zur Verschleierung vor Sicherheitsmechanismen (z. B. Antiviren-Scanner).[2]
- Niedrige Eintrittsschranken in die Cybercrime – durch Cybercrime-as-a-Service werden kaum technische Kenntnisse zur Begehung einer Cyber-Straftat benötigt.

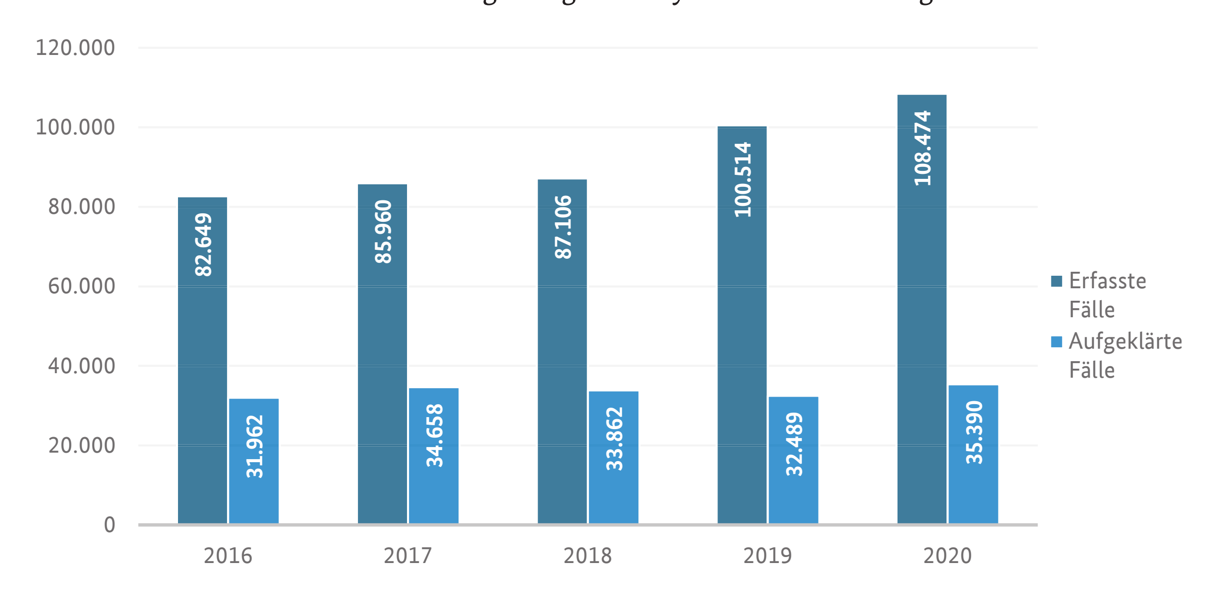


Abbildung 6: Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen Deutschland von 2016 bis 2020

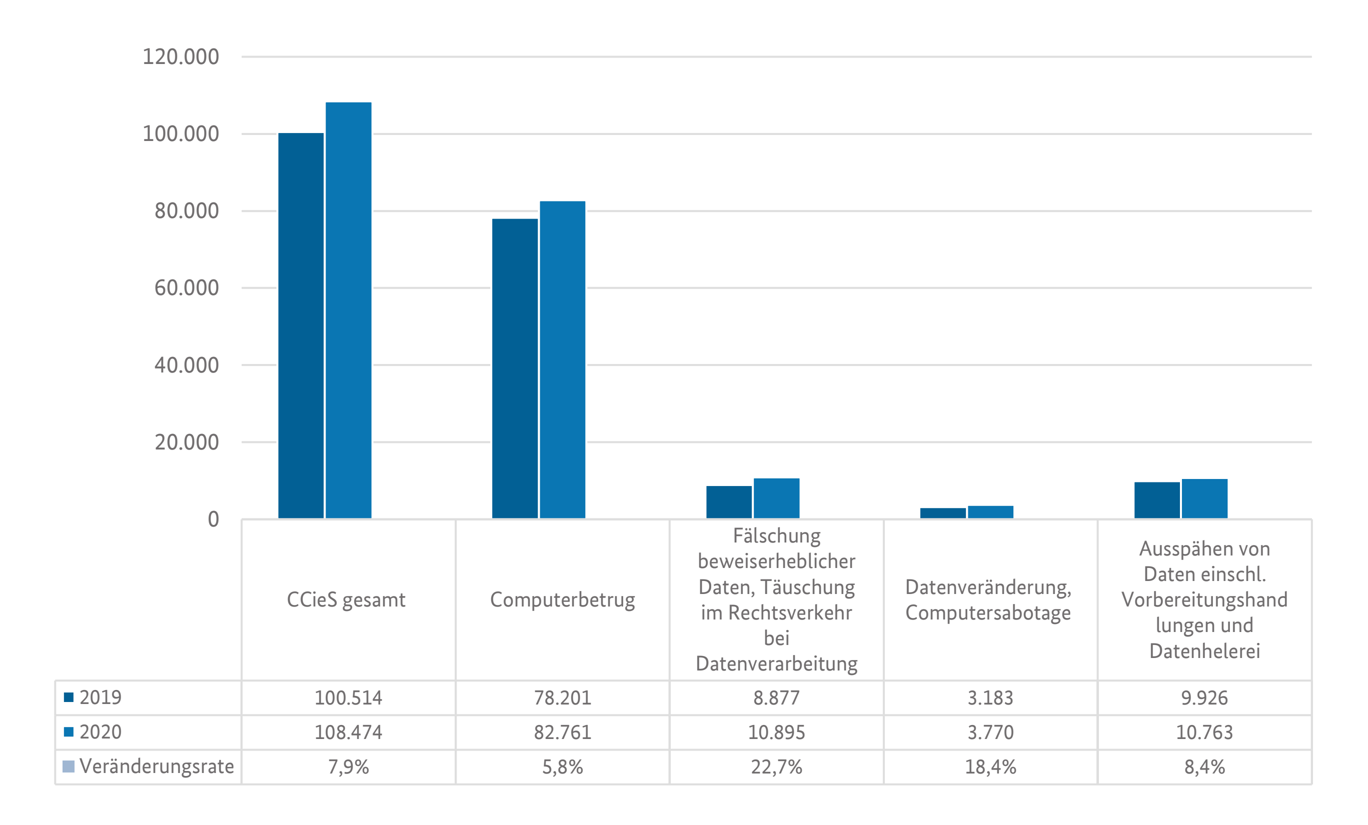
	Anzahl erfasster Fälle (absolut)	Absolute Differenz erfasster Fälle	Prozentuale Differenz erfasster Fälle	Aufgeklärte Fälle (absolut)	Aufgeklärte Fälle Differenz (absolut)	Aufgeklärte Fälle in %, Aufklärungs-Quote (AQ)	Prozentuale Differenz der AQ
2016	82.649			31.962		38,7 %	
2017	85.960	3.311	4,01 %	34.668	2.696	40,3 %	1,6 %
2018	87.106	1.146	1,33 %	33.862	-796	38,9 %	-1,4 %
2019	100.514	13.408	15,39 %	32.489	-1.373	32,3 %	-6,6 %
2020	108.474	7.960	7,92 %	35.390	2.901	32,6 %	0,3 %

Abbildung 7: Erfasste und aufgeklärte Fälle (absolute und prozentuale Angaben inkl. der jeweiligen Aufklärungsquote) in Deutschland von 2016 bis 2020 – Tabellenübersicht

Wie in den Abbildungen ersichtlich, steigt die Anzahl der erfassten Fälle kontinuierlich, während sich die der aufgeklärten Fälle im Bereich von 31.000 bis ca. 35.000 bewegt. Die Folge ist eine Absenkung bzw. Stagnation der Aufklärungsquote.

[2] Obfuskationsfähigkeiten

Folgende Abbildung zeigt das Fallaufkommen ausgewählter Straftaten der Cybercrime im engeren Sinne. Auch hier zeigt sich der Anstieg der Fallzahlen in einzelnen relevanten Deliktsfeldern:



	CCieS gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei
2019	100.514	78.201	8.877	3.183	9.926
2020	108.474	82.761	10.895	3.770	10.763
Veränderungsrate	7,9%	5,8%	22,7%	18,4%	8,4%

Abbildung 8: Fallaufkommen von Straftaten der CCieS 2019 und 2020

4 Relevante Phänomenbereiche der Cybercrime

4.1 DIE UNDERGROUND ECONOMY – MARKTPLÄTZE IM CYBERRAUM

Die Gesamtheit aller täterseitig illegal genutzten Plattformen werden aufgrund ihrer starken wirtschaftlichen Ausrichtung als „Underground Economy“ bezeichnet.



Die Underground Economy ...

... ist ein krimineller Spiegel der realweltlichen und globalisierten Gesellschaft - Angebot und Nachfrage beherrschen den kriminellen Markt, der stetig wächst.

Das System ...



... basiert auf arbeitsteiligen Wertschöpfungsketten, losen interpersonellen Strukturen und vornehmlich finanzieller Motivation. Es bildet auf dieser Grundlage ein international vernetztes, organisiertes und in sich logisches, kriminelles Konzept.



Beliebte Handelsware: Digitale Identitäten

Mit Stand 16.02.21 zählte die Webseite "HaveIBeenPwnd" rund 10.594.333.080 identifizierte kompromittierte Accounts – das Hasso-Plattner-Institut sogar 12.211.907.424. Letztere kommen hierbei auf 1.635.908 geleakte Accounts pro Tag. Jeder gestohlene Datensatz kann wiederum als Ausgangspunkt für weitere kriminelle Handlungen genutzt werden.

Abbildung 9: Die wesentlichen Aspekte der Underground Economy – weiterführende Links zu Statistiken abgeflossener Daten finden sich hier: *https://haveibeenpwned.com/* und *https://sec.hpi.de/ilc/?lang=de*

4.1.1 Cybercrime-as-a-Service (CCaaS)

Cybercrime-as-a-Service (Cyberstraftat als Dienstleistung) nimmt einen enormen Stellenwert in der Cybercrime ein und gewinnt stetig an Relevanz. CCaaS basiert auf der professionellen, lose strukturierten, arbeitsteiligen sowie am finanziellen Gewinn orientierten kriminellen Gemeinschaft der Underground Economy. Die damit einhergehende Zergliederung und Globalisierung führt zu einer steigenden Spezialisierung der einzelnen CCaaS-Anbieter und versetzt auch weniger cyberaffine Straftäter in die Lage, aus technischer Sicht komplexere Straftaten und Angriffsmodi zu realisieren.

Das Cybercrime-as-a-Service-Modell basiert dabei auf neun Säulen (s. Appendix S. 46). Diese decken den gesamten Verlauf einer kriminellen Tat ab, beginnend von der Suche nach Services und dem Anmieten von Servern, über das Einkaufen von digitalen Identitäten, dem Programmieren und „Abhärten“ von Malware, ihrem „Crashtest“ gegen gängige Anti-Viren-Software bis hin zu deren Distribution, der Profiteintreibung und digitalen Geldwäsche.

Durch das Outsourcing auf „inkriminierte Dienstleister“ können Cybertäter die technische Komplexität ihrer Tatbegehungen weiter erhöhen. Dabei werden auch grundsätzlich legale und kommerzielle Tools, wie etwa die Software Cobalt Strike (s. Abbildung Nr. 10), für kriminelle Zwecke missbraucht.



Abbildung 10: Kaufangebot der Software „Cobalt Strike“ [3]

4.1.2 Angebote im Darknet

Folgende, rein exemplarische Auflistung verdeutlicht, in welcher preislichen Spanne sich Angebote digitaler Identitäten und krimineller Services bewegen:

Service	**Preis in US $** (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ Desktop-Version	1.000 - 10.000 $	bei Kauf
▪ Mobile-Version	1.000 - 10.000 $	bei Kauf
RAT	89 - 530 $	pro Monat bei Miete
(Remote Administration Tool)	Ca. 3.000 $	bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	20 - 100 $	bei Kauf von einem Crypt
	360 - 500 $	bei einem Wochen-Abo mit 50 Crypts pro Tag
Spam	10 ct - 4 $	pro Spam
DDoS as a Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ Shared	5 - 50 $	pro Monat bei Miete
▪ Dedicated	50 - 700 $	pro Monat bei Miete

Abbildung 11: Übersicht krimineller Services im Darknet

[3] Bei Cobalt Strike handelt es sich um eine Software, welche zur Simulation von Angriffen auf das eigene Netzwerk und dadurch Schließung von Sicherheitslücken erworben werden kann.



Abbildung 12: Kaufangebot für Crypting

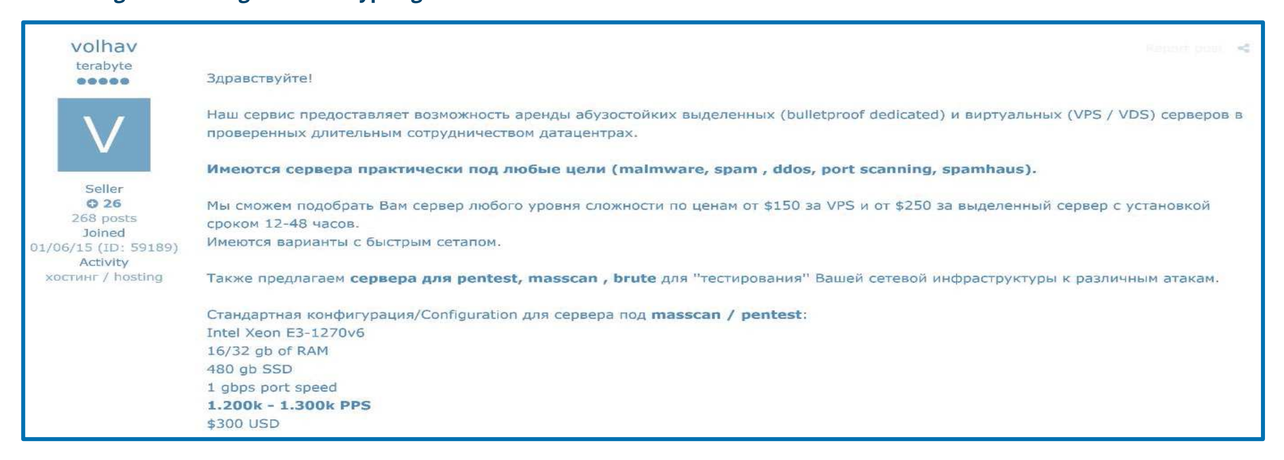


Abbildung 13: Kaufangebot für Bullet Point Hosting

Insbesondere im Zusammenhang mit der Corona-Pandemie und der Entwicklung erster Impfstoffe hat sich auch das Angebot in der Underground Economy entsprechend angepasst.
Dabei konnten diverse Marktplätze festgestellt werden, die vermeintliche Angebote zum Verkauf der medial bekannten Impfstoffe bewerben. Auch wenn authentische Angebote nicht vollständig ausgeschlossen werden können, ist der Großteil der Angebote **als unglaubwürdig zu bewerten.**



Abbildung 14: Screenshots zu Angeboten von Fake-Impfstoffen im Darknet

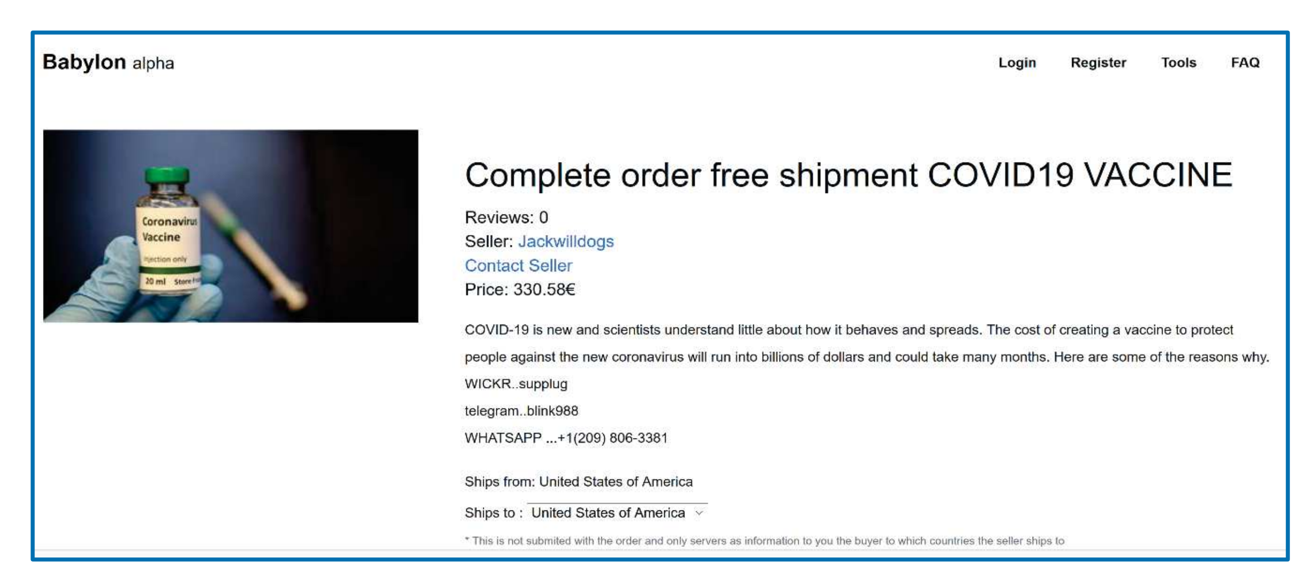


Abbildung 15: Weiterer Screenshot zu einem Angebot eines Fake-Impfstoffes im Darknet

Auf etablierteren Darknet-Marktplätzen konnten schon früh Bestrebungen der Betreiber zum Verbot von Impfstoffangeboten festgestellt werden. Die Durchsetzung dieser „Compliance" wurde teilweise auf vorhandene Scam-Verbote oder explizite Änderungen der Plattformregeln gestützt. Ähnlich wie bei Kinder- und Jugendpornografie, Waffen oder Fentanyl ist hier eine partielle Selbstregulierung zu beobachten, die nicht zuletzt dem kontinuierlichen Strafverfolgungsdruck der letzten Jahre geschuldet ist.

4.2 MAIL-SPAM UND PHISHING: DER TYPISCHE WEG ZU OPFER-DATEN

Um an digitale Identitäten zu gelangen, setzten Cyberkriminelle auch in 2020 auf altbekannte Methoden, allen voran Spam-Mail-Kampagnen und professionelle Phishing-Mails mit maliziösen Office-Anhängen.

Der Spamversand kann über zuvor kompromittierte oder aber kommerziell angemietete Serverkapazitäten sowie über von Angreifern gestohlene legitime E-Mail-Accounts stattfinden. Auch das aggressive Eindringen in ein System via Brute-Force-Angriff auf mangelhaft geschützte Remote-Desktop-Protokolle (RDP) ist ein beliebter Eintrittsvektor in Zielsysteme. Über diese werden wiederum Schadprogramme oder missbräuchlich eingesetzte Pentesting-Tools[4] eingeschleust. In Folge dessen werden Daten ausgespäht und an die Täter weitergeleitet.

[4] Penetrationstests prüfen die Vulnerabilität von IT-Systemen gegenüber Angriffen. Sie sind grundlegender Bestandteil von IT-Sicherheits- und Schwachstellenanalysen.



Eintrittsvektoren

Spam-Mail, maliziöse Anhänge, Fake-Webseiten oder RDP-Kompromittierung



Diebstahl der Daten

Einsatz von Malware und Tools



Exfiltration

Weiterleitung der Daten und missbräuchliche Verwendung

Abbildung 16: Mail-Spam und Phishing

Dieser simpel erscheinende Ablauf sowie der Einsatz bereits bekannter Angriffsarten bleibt weiterhin ein elementarer Bestandteil der Cybercrime. Besonders gefährliche Malware-Familien (Schadprogramme) wie „Emotet" und „Trickbot" sowie einige Ransomware-Familien werden via E-Mail distribuiert. Die dadurch entstehende Sicherheitslücke kann zu einer Gefahr werden und schwerwiegende Folgen für die Betroffenen mit sich bringen.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) erhebt fortlaufend die sogenannten Abwehr-Indizes, die das Aufkommen und die Entwicklung von Malware-Angriffen per E-Mail auf die Netze des Bundes sowie die Menge präventiver Sperrungen von maliziösen Webseiten messen. Das Jahr 2018 stellt dabei das Basisjahr dar (Index = 100).

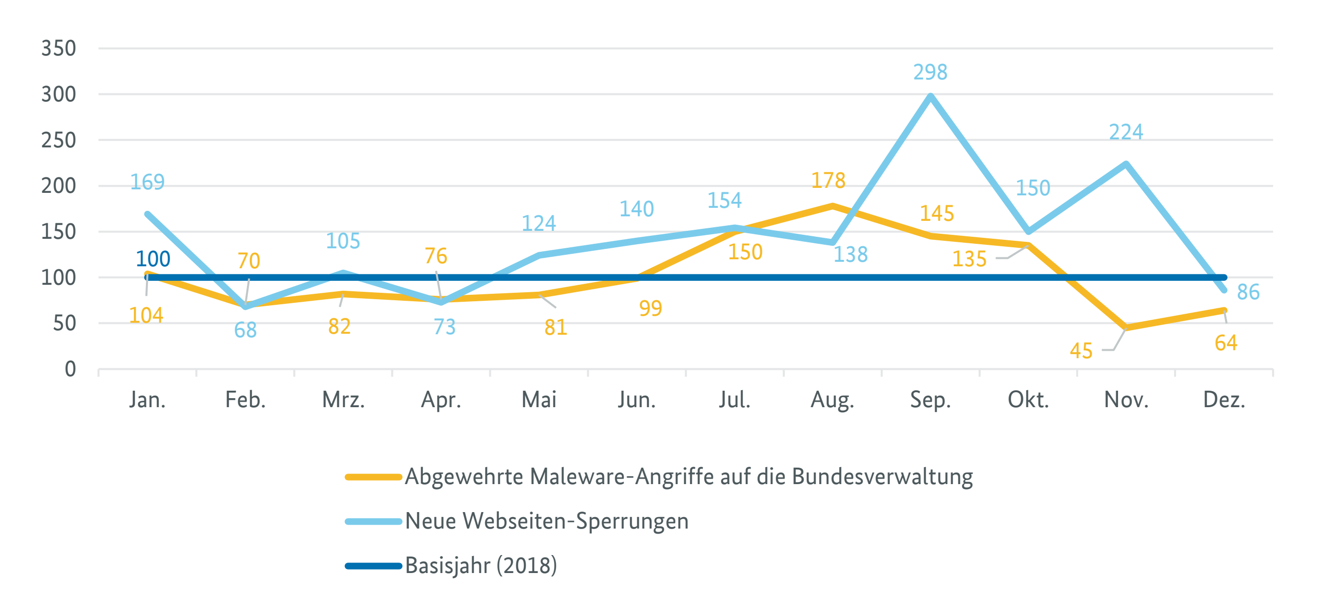


Abbildung 17: Abwehr-Indizes 2020 [5]

Während die Indizes in den Monaten Februar und März 2020 unterdurchschnittlich verliefen, konnte in den Sommermonaten eine erhöhte Aktivität festgestellt werden, welche im Herbst ihren Höhepunkt erreichte. Der Wert für August 2020 stellte hierbei einen Anstieg von 196 % im Vergleich zum Vorjahresmonat dar. Folglich stieg auch die Anzahl an Website-Sperrungen an, welche ihren Höhepunkt wiederum im September erreichte.

Auch die in den Netzen des Bundes festgestellte Anzahl der Spam-Mails ist Gegenstand regelmäßiger Auswertungen des BSI. Anhand der nachfolgenden Grafik, die vom BSI erstellt

[5] Bundesamt für Sicherheit in der Informationstechnik

bzw. die auf dessen Daten beruht, ist mit Ausnahme der Sommermonate Juni bis August ein leichter Anstieg bei der Zahl der Spam-Mails im Vergleich zu den Durchschnittswerten aus 2018 erkennbar. Insgesamt stieg das durchschnittliche Spam-Mail-Aufkommen in 2020 um 17 %.

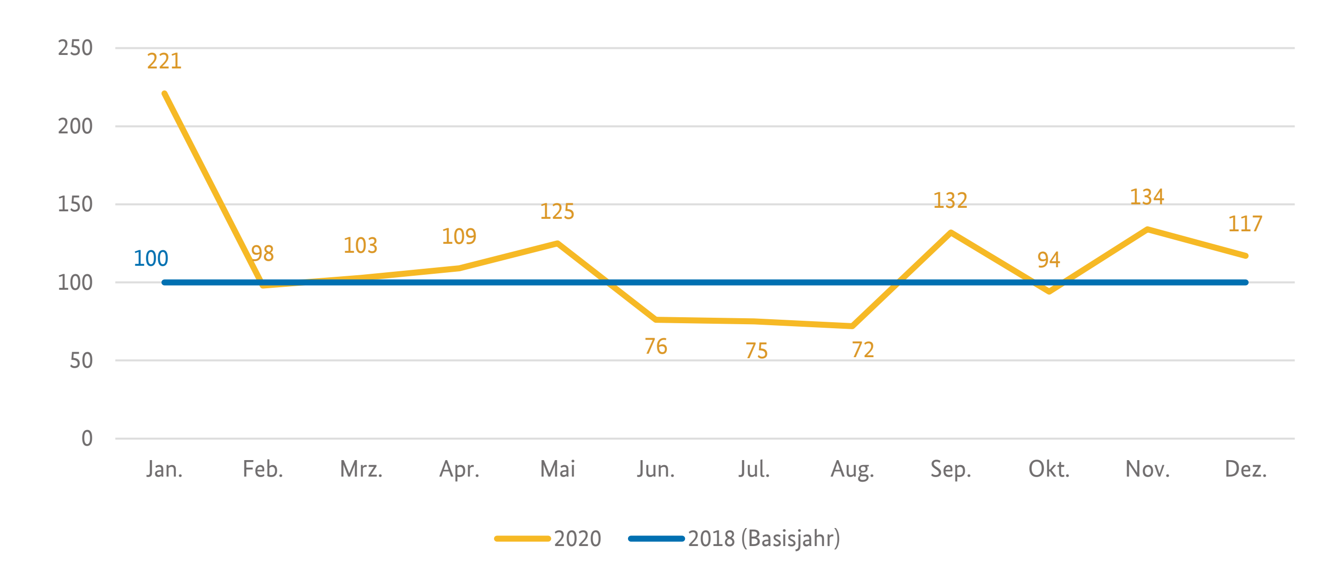


Abbildung 18: Spam-Mail-Index 2020 [6]

Diebstahl digitaler Identitäten - Neuer Modus Operandi im Bereich Mobile Payment



Im Jahr 2020 wurden erstmals Betrugsstraftaten im Zusammenhang mit Mobile Payment festgestellt.

Bargeldlose Bezahlungen mittels Kreditkarten sollen durch die Nutzung sogenannter Token und das Abspeichern der dazugehörigen Daten einzig auf den Token-Servern effektiver und sicherer werden.

Allerdings ist es ab 2020 Tätern gelungen, über Phishing und Social Engineering an für das Online-Banking notwendige Daten zu gelangen und im weiteren Verlauf der Tathandlungen sog. One Time Passwords, die z. B. für den Implementierungsprozess (Enrolement) von Kreditkartennummern in Apple Pay und Google Pay erforderlich sind, zu aktivieren und anschließend betrügerisch einzusetzen.

Nach erfolgreicher Übertragung der Token auf die Täter-Smartphones erfolgte der betrügerische Einsatz auf drei verschiedene Arten:

Die Täter nutzen die Bezahlfunktion des Smartphones an POS-Terminals vor Ort bei unterschiedlichen Vertragsunternehmen mittels NFC zur betrügerischen Erlangung von Waren.

Die Kreditkartennummer-Token werden zur Bezahlung von Online-Einkäufen genutzt (sogenannter e-commerce bzw. card not present fraud).

Apple Pay / Google Pay wird zur Aufladung von Bankkonten über die App von Online-Banken genutzt. So sind die Täter in der Lage, über von Finanzagenten eröffnete Konten an Bargeld bzw. Buchgeld zu gelangen.

[6] Bundesamt für Sicherheit in der Informationstechnik

Im Sommer 2020 wurden vermehrt betrügerische Transaktionen zum Nachteil diverser deutscher kartenausgebender Banken festgestellt. Diese fanden mit Schwerpunkt in Italien, Polen und im Internet statt. Mit Stand November 2020 belief sich die Summe der missbräuchlichen Transaktionen auf ca. 85.000 €, wobei weitere missbräuchliche Umsätze in Höhe von ca. 93.000 € durch die Kartenorganisationen abgelehnt wurden.

4.3 MALWARE

Der Einsatz von Malware ist und bleibt elementarer Bestandteil der CCieS – kaum eine Straftat wird ohne Malware oder missbräuchlich eingesetzte Tools begangen.

Die Bandbreite an Funktionalitäten der bekannten Malware-Familien ist äußerst groß.
In der folgenden Liste werden die am häufigsten eingesetzten Malware-Arten vorgestellt:

Downloader (bzw. Dropper/ Loader)

- Dient primär als "Einfallstor": Setzt sich im infizierten System fest und lädt weitere Arten von Malware nach.
- *Beispiel: Emotet*

Information-Stealer

- Stehlen alle möglichen Arten von Daten über das infizierte System z. B. digitale Identitäten, Passwörter, Online-Banking-Daten etc. Können ebenfalls die Aufzeichnung von Tastaturanschlägen und die unberechtigte Aufnahme von Screenshots umfassen.
- *Beispiel: Trickbot, Qbot, Gootkit*

Ransomware

- Verschlüsselt das System und erpresst damit das Opfer.
- Zur Entschlüsselung wird eine digitale Lösegeldsumme gefordert, die an die Täter gezahlt werden soll.
- *Beispiel: Doppelpaymer, Ryuk, Sodinokibi, Conti, Maze*

Adware

- Software, welche ungewollte Werbeinhalte anzeigt. Im Vergleich zu anderen Varianten von Schadsoftware werden im Normalfall keine Funktionen des Betriebsgerätes beeinträchtigt.
- *Beispiel: Silver Sparrow*

(Krypto-)Miner

- "Schürfen" auf fremden Systemen ohne Wissen des Besitzers nach Kryptowährungen. Dadurch wird illegitim Rechenleistung des infizierten Systems in Anspruch genommen.
- *Beispiel: XMRig, Black Squid*

Mobile Malware

- Wird speziell für mobile Endgeräte entwickelt. Besonders häufig handelt es sich bei Mobile Malware um Adware oder Info-Stealer.
- *Beispiel: Agent Smith*

Pentesting- und Remote Access Tools

- Keine Malware im eigentlichen Sinn, sondern missbräuchlich eingesetzte, oftmals kommerzielle Tools, welche den Fernzugriff auf Systeme erlauben oder dem Pentesting dienen.
- *Beispiel: Mimikatz, CobaltStrike*

Abbildung 19: Darstellung typischer Malware-Arten

4.3.1 Malware in Zahlen

Die folgenden Daten beziehen sich auf Angaben des IT-Sicherheitsdienstleisters AV-Test[7]:

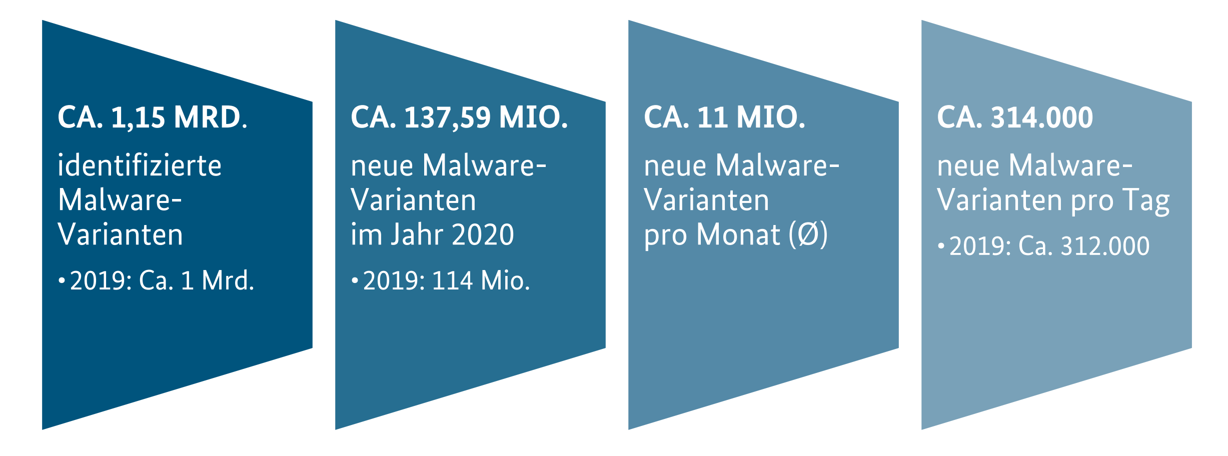


Abbildung 20: Malware-Statistiken 2020 von AV-Test

[7] Vgl. https://www.av-test.org/de/statistiken/malware/

4.3.2 Die globale Malware-Wertschöpfungskette



Abbildung 21: Darstellung der kriminellen Wertschöpfungskette durch Malware-Attacken

4.3.3 Fallbeispiel Malware – Ausnutzen einer Schwachstelle

Platzierung von Kryptominern auf Systemen in einzelnen Ämtern der Stadtverwaltung Potsdam und Brandenburg an der Havel

Am 22.01.20 wurde der Zentralen Ansprechstelle Cybercrime (ZAC) der Polizei des Landes Brandenburg gemeldet, dass mehrere Server der Stadtverwaltung Potsdam kompromittiert worden sind. Dieser IT-Sicherheitsvorfall führte dazu, dass mehrere Server einzelner Ämter der Stadtverwaltung Potsdam abgeschaltet wurden. Unter anderem waren Onlinefunktionen der örtlichen Straßenverkehrs- und Zulassungsbehörde teilweise für einige Wochen nicht nutzbar. Bereits am 23.02.20 gab es eine ähnliche Meldung der Stadtverwaltung Brandenburg an der Havel, jedoch mit weniger betroffenen Systemen.

Untersuchungen des zentralen IT-Dienstleisters des Landes Brandenburg und eines externen Dienstleisters führten zu dem Ergebnis, dass durch unbekannte Täter eine Schwachstelle in der „Citrix-Anwendung“ ausgenutzt und ein „Kryptominer“ für die digitale Währung Monero installiert werden konnte.

4.3.4 Angriffe auf Geldautomaten mittels Malware

Bei logischen/digitalen Angriffen auf Geldautomaten kommt oftmals Schadsoftware zum Einsatz. Generell unterscheidet dieser Phänomenbereich drei Modi Operandi:

Jackpotting mit Malware

Angriff auf den Rechner/PC eines Geldautomaten mittels Schadsoftware.

Jackpotting mit Blackbox

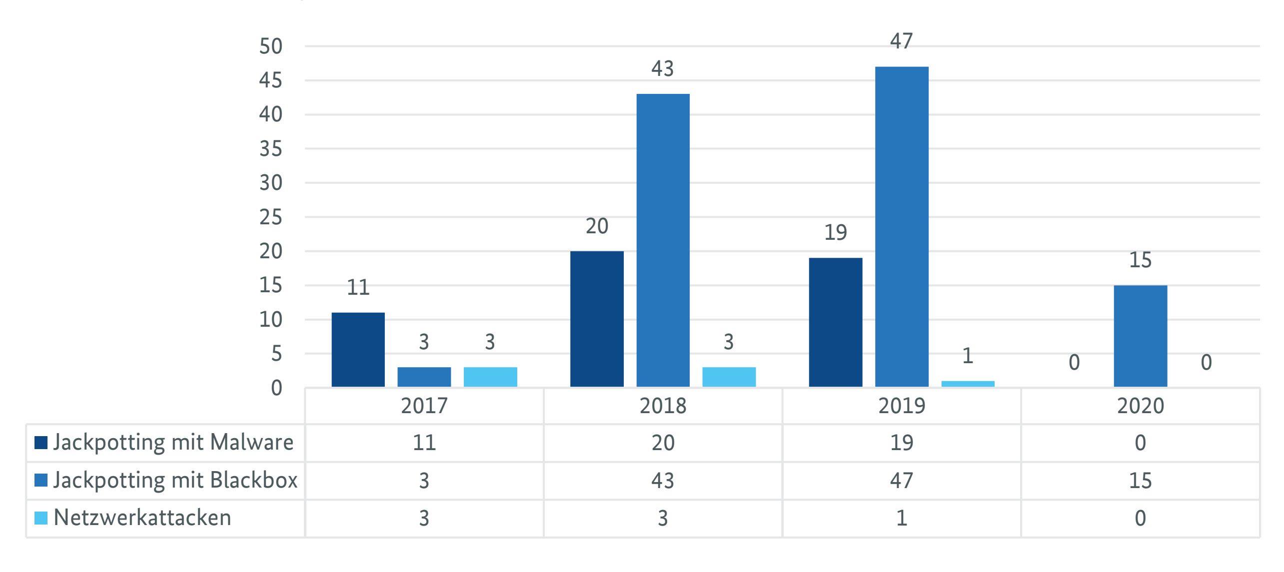
Angriff auf das Auszahlungsmodul des Geldautomaten mittels tätereigener Hardware.

Netzwerkattacke

Malwareangriff auf die kartenausgebende Bank oder Processing-Gesellschaft, um Transaktionsprozesse zu manipulieren; anschließend erfolgt ein sog. kartengebundener „Cash Out" oder Malwareangriff auf die Geldautomaten-betreibende Bank, um einen direkten Zugriff auf die im Netzwerk verbundenen Geldautomaten zu erhalten und einen sog. kartenungebundenen „Cash Out" durchzuführen.

Abbildung 22: Modi Operandi bei logischen/digitalen Angriffen auf Geldautomaten

Im Jahr 2020 wurden keine Fälle von Jackpotting mit Malware oder Netzwerkattacken festgestellt. Zudem kam es in Deutschland zu einem starken Rückgang der Fallzahlen beim Jackpotting mit Blackbox. Lediglich vier der 15 Jackpotting-Angriffe mit Blackbox in Deutschland verliefen im Jahr 2020 erfolgreich. Aufgrund von technischen Sicherheitsvorkehrungen, z. B. Verschlüsselung der Festplatte (Jackpotting) bzw. Verschlüsselung der Kommunikation zwischen dem Geldautomaten-PC und Auszahlungsmodul (Blackboxing) werden die meisten logischen Angriffe auf Geldautomaten abgewehrt.



	2017	2018	2019	2020
Jackpotting mit Malware	11	20	19	0
Jackpotting mit Blackbox	3	43	47	15
Netzwerkattacken	3	3	1	0

Abbildung 23: Fallzahlen logische Angriffe auf Geldautomaten in Deutschland

Die Bedrohungslage ist trotz rückgängigem Fallaufkommen im Bereich der logischen Geldautomaten-Angriffe gegeben. Es kann nicht ausgeschlossen werden, dass der Rückgang der Fallzahlen mit den Reisebeschränkungen der Covid-19-Pandemie zusammenhängt, da in der Vergangenheit die Täter vermehrt aus dem Ausland eingereist sind.

4.4 RANSOMWARE

Ransomware zählte auch im Jahr 2020 zu den primären Bedrohungen für Unternehmen und öffentliche Einrichtungen. Von allen Modi Operandi im Phänomenbereich Cybercrime besitzt Ransomware das höchste Schadenspotenzial. Eine Infektion mit Ransomware und eine damit zusammenhängende Verschlüsselung des Systems kann für jede Art von Unternehmen zu massiven und kostenintensiven Geschäfts- bzw. Funktionsunterbrechungen führen.

Attacken auf KRITIS, z. B. Krankenhäuser und Wasserwerke, zeigen, dass erfolgreiche Ransomware-Angriffe drastische Folgen für die Zivilbevölkerung nach sich ziehen und elementare Services des öffentlichen Geschehens sabotieren können.

4.4.1 Ransomware-Trends 2020



Die Anzahl von Ransomware-Angriffen steigt.



Cyberkriminelle fokussieren sich bei ihren Angriffszielen derzeit verstärkt auf das sog. „Big Game“, also große Unternehmen und öffentlichen Einrichtungen.



Double Extortion avanciert zum Standard-Modus-Operandi:

Hierbei erfolgt die Verschlüsselung der Systeme bei gleichzeitiger Erpressung des Opfers mit Veröffentlichung der abgeflossenen Daten.

Dieses Vorgehen bietet den „Vorteil", dass bei einer Weigerung des Opfers zur Zahlung der Entschlüsselung der Systeme noch aus den ausgeleiteten Daten finanzielle Vorteile generiert werden können.



Laut der im August 2020 publizierten, repräsentativen Umfrage des Forschungsprojektes der IT-Sicherheitsinitiative des BMWi „Cyberangriffe gegen Unternehmen in Deutschland“ ist bei Ransomware-Angriffen ein linearer Anstieg der Betroffenheit mit zunehmender Unternehmensgröße zu erkennen.

Während nur etwa jedes neunte kleine Unternehmen in den vergangenen zwölf Monaten (2018/2019) von mindestens einem Ransomware-Angriff betroffen war, betraf es jedes vierte bis fünfte große Unternehmen.

Abbildung 24: Ransomware-Trends und Highlights. Link zur Studie des Forschungsprojektes „Cyberangriffe gegen Unternehmen in Deutschland“ [8]

---

[8] Die Studie kann hier abgerufen werden: *https://www.it-sicherheit-in-der wirtschaft.de/ITS/Redaktion/DE/Publikationen/cyberangriffe-gegen-unternehmen-in-deutschland.html*

4.4.2 Finanzielle Dimensionen von Ransomware

LÖSEGELD/RANSOM

Die verzeichnete Spannweite liegt gemäß einer Unternehmensbefragung aus 2018/2019 zwischen 10 und 100 Mio. Euro.[a]

Laut IT-Sec-Dienstleister Coveware stiegen die durchschnittlichen Lösegeldforderungen in 2020 weiter an.[b]

SCHÄDEN

Ransomware verursacht einen Schaden im mindestens sechs- bis siebenstelligen Euro-Bereich.

Darin nicht enthalten: Reputationsschäden und Folgeschäden durch den Abfluss sensibler Daten.

KRIMINELLE EINNAHMEN

Laut Chainalysis ist der Profit, den Ransomware-Gruppierungen im Jahr 2020 in Form von Kryptowährungen erfolgreich erpresst haben, um 311 % im Vergleich zum Vorjahr gestiegen.

Abbildung 25: Finanzielle Dimensionen hinsichtlich Ransomware[9]

4.4.3 Ransomware-as-a-Service

Ransomware-Akteure handeln mittlerweile organisiert und arbeitsteilig, sodass sich innerhalb der Underground Economy das Ransomware-as-a-Service-Modell etabliert hat. Dabei programmiert eine Gruppe von Kriminellen eine Ransomware und heuert weitere Operatoren an, die wiederum die Software auf die Zielsysteme laden.

Dank eines Affiliate-Systems profitieren alle Beteiligten: Für jede erfolgreiche Erpressung erhalten die Operatoren einen Teil der erpressten Lösegeldsumme – der Rest fließt den Ransomware-Codern zu.

---

[9] Weiterführende Quellen:
[a] Siehe Fußnote Nr. 8
[b] Coveware: *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#:~:text=Average%20Ransom%20Demand%20Q4%20of%202020&text=The%20average%20ransom%20payment%20decreased,%24110%2C532%2C%20a%2055%25%20reduction.*
[c] Chainalysis: *https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021* und *https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets*

Von der Programmierung über die Erpressung zum Lösegeldeingang

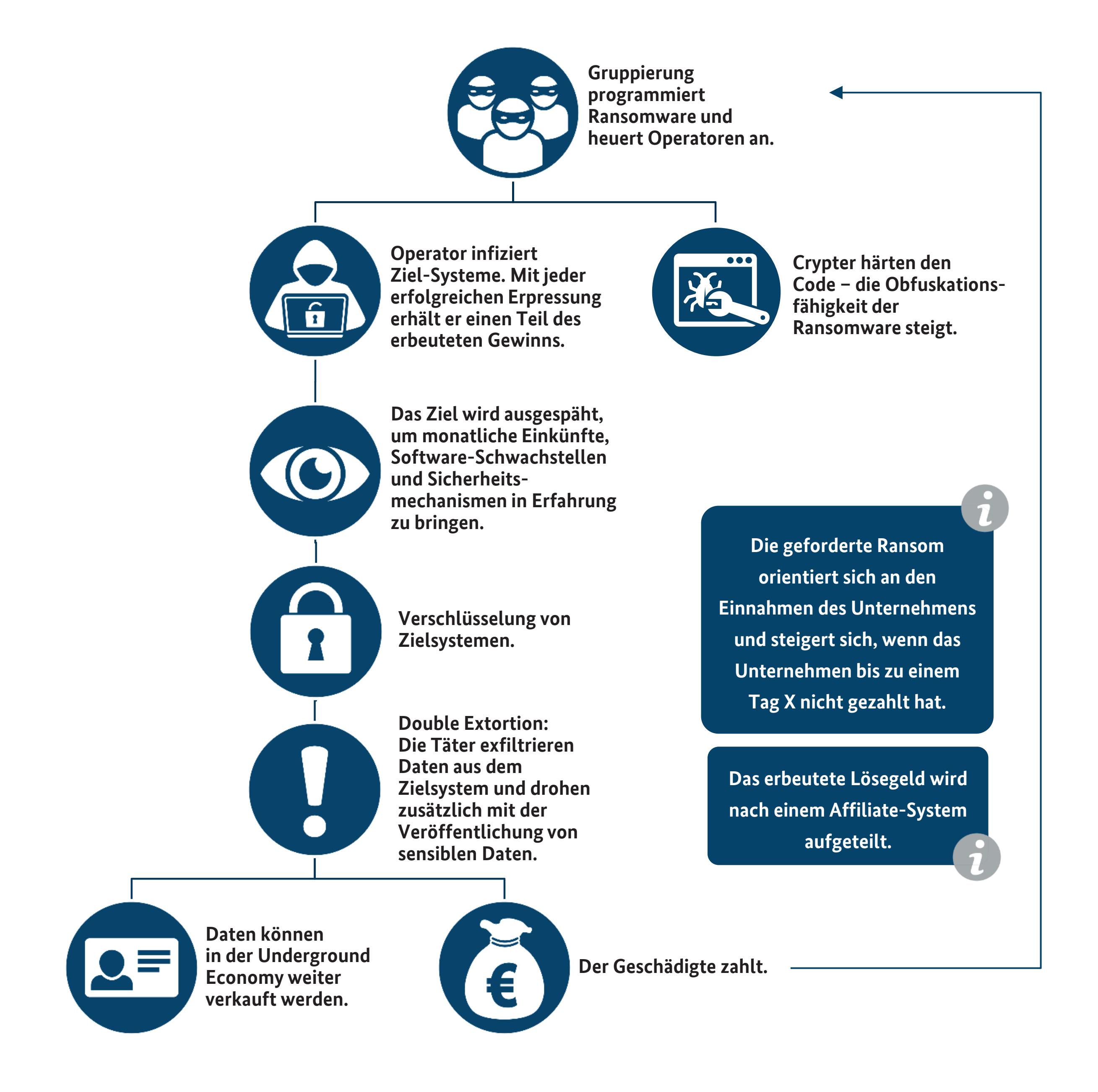


Abbildung 26: Ransomware-Wertschöpfungskette

4.4.4 Aktive Ransomware-Familien in Deutschland (Auszug)

Phobos

Seit 2018 aktiv – besonders häufig bei Angriffen auf kleinere Unternehmen verwendet.

Doppelpaymer

Ausführungen siehe weiter unten.

Avaddon

Wird über Malspam-Kampagnen distribuiert – präferierte vergangene Ziele lagen im US-amerikanischen Bankensektor.

Egregor

Im Februar 2021 wurden mehrere Kunden/ Affiliates der eigentlichen Kerngruppierung durch ukrainische Strafverfolgungsbehörden verhaftet.

Netwalker

Auch bekannt als "MailTo" und "Bugatti" – trat vermehrt im Zuge der COVID-19-Pandemie in Erscheinung.

Cl0p

Mutmaßlich "Ransomware-of-Choice" der Gruppierung "TA505", welche auch in Deutschland Angriffe ausgeführt hatte (s. Kapitel 5.2.1).

Sodinokibi

Besitzt laut IT-Sicherheitsdienstleister Coveware den größten Marktanteil aller Ransomware-Familien.

Nefilim

Präsenz stieg 2020 stark an – u.a. durch eine für Double Extortion typische "Data-Leak"-Seite im TOR-Netzwerk.

Ryuk

Erlangte öffentliche Aufmerksamkeit als favorisierte, nachgelagerte Ransomware bei Emotet-Angriffen.

Die dargestellten Ransomware-Familien stellen nur einige Bestandteile des Ransomware-Kosmos dar.

Die Bandbreite an Ransomware-Familien und die Entwicklungsdynamik sind hoch – Ransomware ist ein internationales Problem, welches sich stets weiterentwickelt und fortlaufend neue Ransomware-Familien hervorbringt.

Sobald eine Ransomware-Gruppierung ihre Aktivitäten einstellt, nimmt eine neue ihren Platz im kriminellen Markt ein.

Abbildung 27: Auflistung in Deutschland aktiver Ransomware-Familien. [10]

[10] Weitere Informationen zu den Ransomware-Familien finden sich u. a. hier: *https://malpedia.caad.fkie.fraunhofer.de/*, *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020* oder hier: *https://attack.mitre.org/software/*

4.4.5 Fallbeispiel: Ransomware – Doppelpaymer

Profil

Doppelpaymer wurde erstmals im Jahr 2019 identifiziert. Seit 2020 wird bundesweit ein verstärktes Aufkommen der Ransomware verzeichnet. Vornehmliche Ziele sind dabei Wirtschaftsunternehmen, aber auch öffentliche Einrichtungen.

Bei Doppelpaymer handelt es sich vermutlich um einen Stamm der sog. Bitpaymer-Familie, welche IT-Systeme dauerhaft verschlüsselt.

Angriffsvektoren

Die Schadsoftware verwendet kompromittierte Windows-Fernwartungs-Protokolle, um in das zu infizierende System geladen zu werden. Dort bedient es sich Exploits, um Benutzerrechte zu erhalten und sich im System bewegen zu können.

Doppelpaymer späht dabei Daten zunächst aus und exfiltriert diese, bevor das System verschlüsselt wird. Anschließend erhält das Opfer eine Lösegeldforderung. Die Gruppierung hinter Doppelpaymer verwendet die vorher ausgeleiteten Daten als Druckmittel gegenüber den Opfern, indem mit einer Veröffentlichung gedroht wird (Double Extortion).

Angriffe u. a. auf das Universitätsklinikum Düsseldorf

Verschiedene Firmennetze waren in 2020 Opfer von Doppelpaymer – hierunter auch KRITIS-Unternehmen und DAX-Konzerne. So wurde am Morgen des 10.09.20 die IT-Infrastruktur des Universitätsklinikums Düsseldorf von einer Ransomware-Attacke getroffen.
Durch die Verschlüsselung bildgebender Systeme konnte die zentrale Notversorgung nicht mehr sichergestellt werden, sodass Patienten auf umliegende Krankenhäuser verteilt werden mussten. Von den Tätern wurden vor der Verschlüsselung der Systeme vermutlich 100.000 Patientendaten aus dem Netzwerk entwendet.

4.5 DDOS

DDoS-Angriffe zielen grundsätzlich darauf ab, eine Überlastung des Zielsystems herbeizuführen und verursachen so gezielt Schäden bei den angegriffenen Personen und Organisationen/ Unternehmen. Sowohl in Bezug auf die Anzahl als auch die Intensität war in den letzten Jahren eine stete Steigerung bei den DDoS-Angriffen erkennbar.

Im Jahr 2020 verzeichneten die Unternehmen Link11 und Deutsche Telekom AG (DTAG), beide Kooperationspartner des BKA, eine Steigerung insbesondere hinsichtlich der Anzahl von hochvolumigen DDoS-Angriffen. Wie in Abbildung 29 ersichtlich, stellt Link11 hinsichtlich der Gesamtzahl an DDoS-Angriffen eine teils massive Steigerung ab März bis August fest.

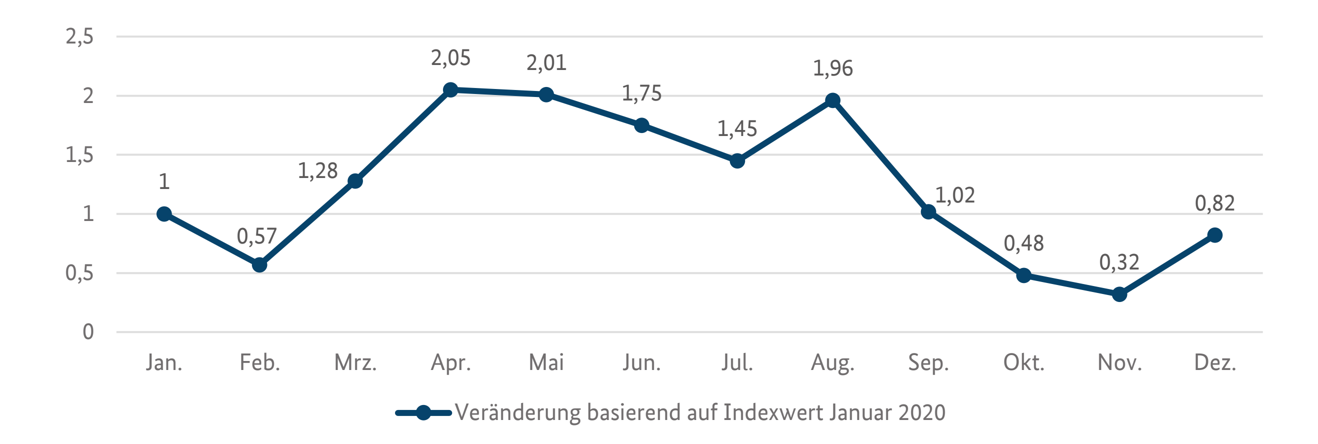


Abbildung 28: Indexwerte DDoS-Angriffe 2020 pro Monat in Deutschland (Basiswert = Januar 2020 mit Wert 1) [11]

Der DDoS-Report 2020 von Link11 enthält ferner folgende Parameter, die bei der Analyse der Angriffe festgestellt werden konnten:

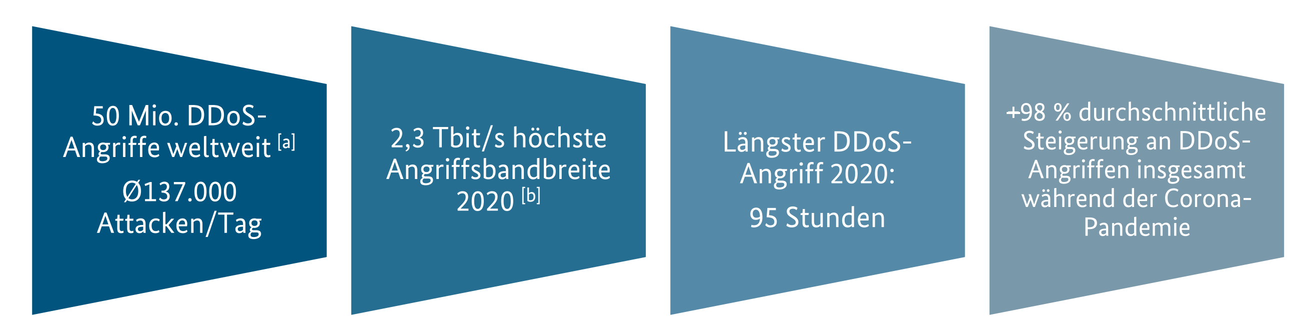


Abbildung 29: DDoS Parameter aus dem Report 2020 von Link11 [12]

Die DTAG stellte bezogen auf Deutschland im Jahresvergleich folgende Angriffsparameter fest:

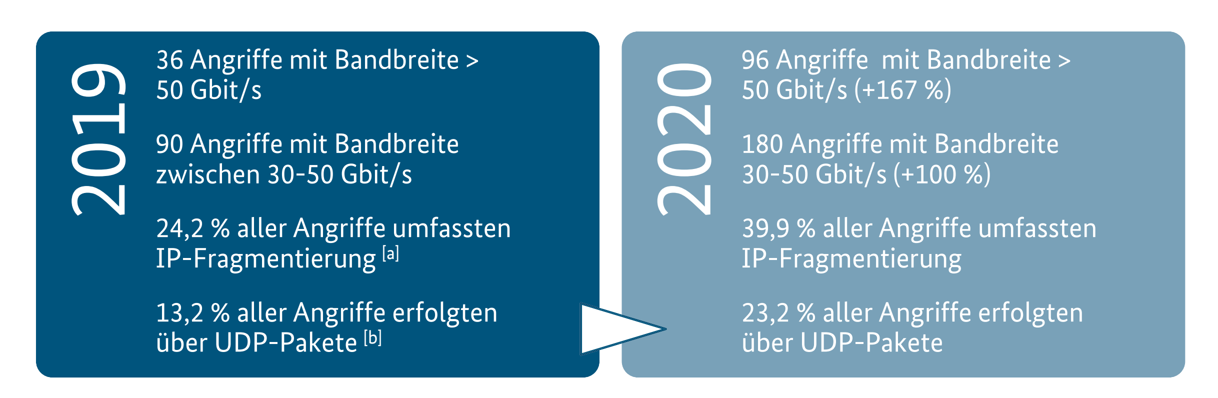


Abbildung 30: Angriffsparameter – Jahresvergleich zwischen 2019 und 2020 [13]

---

[11] [a] Hochrechnung durch Link11 SOC
[b] AWS Meldung zur Netzwerküberwachung

[12] DDoS Report 2020 von Link11

[13] [a] Kommunikation im Internet erfordert die Aufteilung von Datenpaketen.
Der Angriff verhindert das Zusammensetzen der Nachricht durch das Zielsystem
[b] Überforderung von Opfersystemen durch UDP-Pakete (User Datagram Protocol/verbindungsloses Netzwerkprotokoll)

Insbesondere im ersten Corona-bedingten Lockdown konnte seitens der DTAG ein massiver Anstieg an hochvolumigen Angriffen festgestellt werden. Die Corona-Pandemie diente offensichtlich auch in diesem Phänomenbereich als Katalysator für Cyberangriffe.

DDoS-Angriffe (oder deren Androhung) erhielten während der durch die Pandemie forcierten Verlagerung von Arbeiten ins Homeoffice insgesamt ein höheres Bedrohungs- und Schädigungspotenzial. Dabei sind DDoS-Angriffe spätestens seit dem zweiten Lockdown im November 2020 ein einzukalkulierendes Risiko nicht nur für Unternehmen, sondern auch für das Schulwesen, insb. mit Blick auf Home-Schooling.

Die folgende Grafik der DTAG gibt einen Jahres-Überblick über die in Deutschland festgestellten DDoS-Angriffsbreiten:

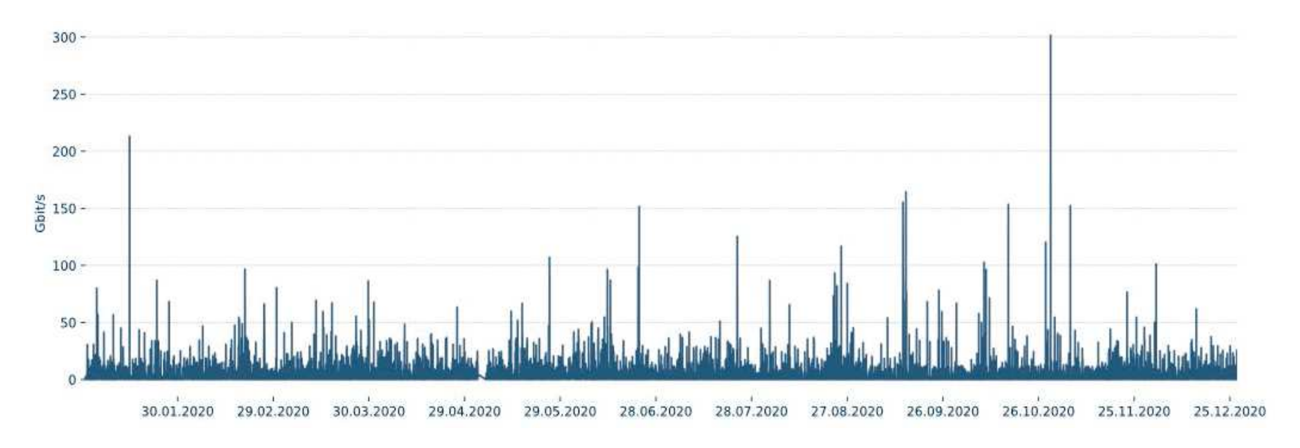


Abbildung 31: DTAG - Maximale Angriffsbreiten von DDoS-Angriffen im Jahr 2020 in Deutschland [14]

Der Großteil der Angriffe erfolgte in 2020 demnach mit einer Bandbreite von bis zu 10 Gbits/s. Laut Auskunft DTAG haben sich die Angriffsbandbreiten über 30 Gbits/s mehr als verdoppelt. Die maximale Bandbreite lag in dem Berichtsjahr bei 301,6 Gbits/s.

Regionale Schwerpunkt von Ziel- und Herkunftsländern von DDoS-Attacken konnten anhand der Auswertung der DTAG nicht getroffen werden; vielmehr ließ sich eine weltweite Verteilung der involvierten Systeme feststellen. Begründung hierfür dürfte sein, dass die Täter für DDoS-Angriffe häufig Botnetze einsetzen und die eingebundenen Bots unabhängig von der Kommandostruktur des Netzes vielfach länderübergreifend verteilt sind. Generell gilt: Dort, wo viele Rechner bzw. internetfähige Geräte zu finden sind, existieren auch vergleichsweise viele Bots, die als Ausgangspunkt von DDoS-Angriffen dienen können.

[14] Deutsche Telekom AG

5 Angriffe auf die Wirtschaft

5.1 BIG GAME HUNTING

Cyberkriminelle greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt. Besonders wirtschaftlich starke Unternehmen, KRITIS und öffentliche Einrichtungen (z. B. Krankenhäuser), welche unter dem Begriff „Big Game" zusammengefasst werden, sind hoch gefährdet. Die Täter wissen um die Notwendigkeit, den reibungslosen Betrieb derartiger Einrichtungen gewährleisten zu können, da diese für die Gesellschaft kritische Dienstleistungen anbieten. Ein Angriff auf derartige Einrichtungen zielt auf ihre Relevanz ab, da ein Ausfall eine gesellschaftliche Notlage bedeuten könnte.

Ziel

Cyberkriminelle greifen zielgerichtet und vermehrt wirtschaftlich starke Unternehmen, KRITIS und öffentliche Einrichtungen an.

Die Notlagen, welche durch den Ausfall dieser Einrichtung entstehen können, werden skrupellos in Kauf genommen.

Motivation

Auch wenn politisch motivierte Cybercrime weiterhin einen hohen Stellenwert einnimmt, bleibt die Hauptmotivation von Cyberkriminellen finanzieller Natur.



Eintrittsvektoren

Die beliebtesten Eintrittsvektoren bleiben (Spear-)Phishing, Malspam, kompromittierte RDP-Protokolle sowie die Nutzung illegitim erlangter Log-In-Daten.

Auch die Ausnutzung von CVE/Exploits dient Tätern als Einfallstor in IT-Systeme.



Abbildung 32: Parameter des Big Game Hunting durch organisierte Cyber-Akteure

Auch im Jahr 2020, in dem vor allem dem Gesundheitswesen eine besondere Bedeutung zukam, konnte eine Intensivierung des „Big Game Hunting" festgestellt werden.

Einer der größten Cyberangriffe in der Geschichte: Die Kompromittierung von SolarWinds „Orion".

Am 13.12.20 wurde bekannt, dass bislang unbekannte Angreifer die Software „Orion"[15] des US-amerikanischen Technologie-Unternehmens „SolarWinds" nach einem dortigen Netzwerkeinbruch derart kompromittiert haben, dass im Zuge der regelmäßigen, unternehmensseitigen Softwareaktualisierung persistent Zugriff auf die IT-Netzwerke der Kunden möglich war.[16] Dabei wurde über die Malware „SUNBURST" eine Backdoor in den infizierten Systemen hinterlassen:

Die Verteilung der schadhaften Updates begann bereits im März 2020. Die Kommunikation mit Command-and-Control-Servern wurde als legitime Kommunikation der Orion-Software getarnt, erlangte Daten in legitimen Konfigurationsdateien zwischengespeichert.

[15] Bei Orion handelt es sich um eine IT-Management und -Monitoring-Software, die weltweit eingesetzt wird.
[16] Ein derartiges Vorgehen bezeichnet man als Supply-Chain-Angriff. Er konzentriert sich auf die Kompromittierung der Lieferkette, um ein Ziel indirekt anzugreifen.

Zeitlicher Ablauf des Angriffs auf SolarWinds „Orion“

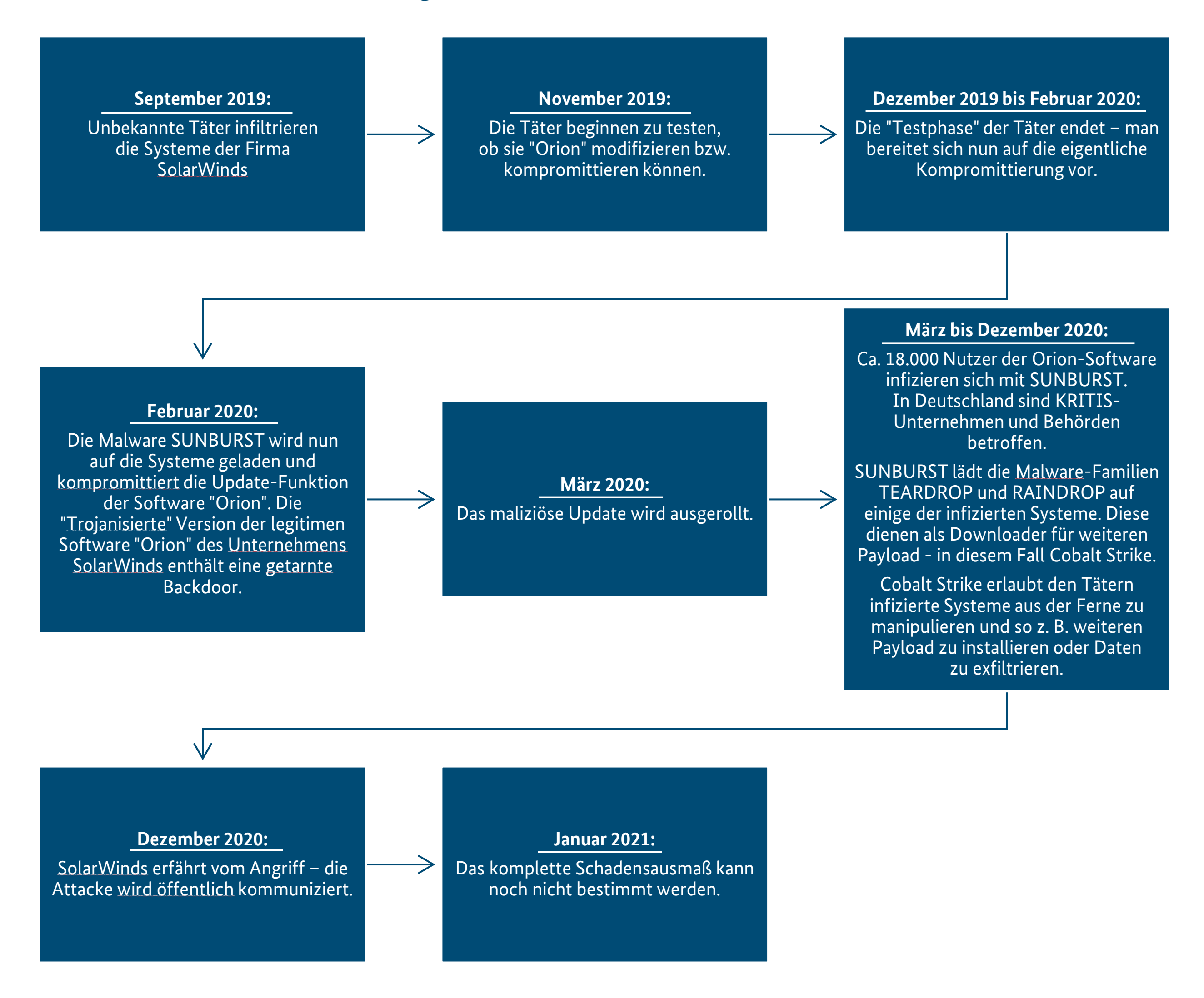


Abbildung 33: Chronologische Darstellung des Supply-Chain-Angriffes auf die Software "Orion" [17]

Die Kompromittierung von „Orion“ wird medial zu den bisher größten und schwerwiegendsten Cyberangriffen der Geschichte gezählt. Die Dimension der Tat spricht für sich: Weltweit waren über 18.000 Systeme betroffen, darunter KRITIS und Behörden. Die Supply-Chain-Attacke zeugt nicht nur von einem professionellen, sondern auch von einem organisierten und vernetzen Vorgehen der Täterschaft.

Der Fall zeigt eindrucksvoll, wie schnell Cyberangriffe durch die Vernetzung und gleichzeitige Ausnutzung von Lieferketten Dimensionen mit großer Reichweite annehmen können.
Dabei müssen Cyberkriminelle nicht mehr unbedingt ihr eigentliches Ziel direkt angreifen: Durch die Verflechtung von Wirtschaftskreisläufen, IT-Systemen und Lieferketten genügt es häufig, jenes Element in diesem Beziehungsgeflecht anzugreifen, dass über die meisten Verbindungen in andere Systeme verfügt.

Der Angriff verdeutlicht die Vulnerabilität, welche durch die voranschreitende Globalisierung wichtiger Player und ihrer Systeme hervorgerufen wird.

---

[17] Weiterführende Quellen:
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/ oder
https://www.heise.de/news/Sunspot-und-Raindrop-Weitere-Malware-der-SolarWinds-Angriffskette-entdeckt-5030754.html

5.2 ADVANCED PERSISTENT THREATS (APT)[18]

APT-Aktivitäten im Jahr 2020

Angriffe auf Behörden, das Finanzwesen, den Gesundheitssektor sowie unternehmensstarke Firmen zeigen, dass Deutschland Aktionsraum und gleichzeitig ein beliebtes Ziel von APT und professionellen, organisierten Gruppen der Cybercrime ist. Deutschland fungiert nicht nur als ein beliebter Server-Standort für kriminelle Infrastrukturen, sondern ist auch ein äußerst wichtiger gesamteuropäischer Wirtschaftsstandort und demzufolge von politischer Relevanz.

Das Verhalten der APT änderte sich in 2020 zwar nur geringfügig, allerdings sehr effektiv – auch hier wurde die Corona-Pandemie für kriminelle Zwecke missbraucht:



Abbildung 34: Charakteristika von APT im Jahr 2020

5.2.1 Fallbeispiele: APT 32, WIZARD SPIDER, TA505

In 2020 waren unter anderem nachfolgende Cyberakteure in Deutschland aktiv. Sie stellen einen Ausschnitt der Gruppierungen dar, welche politisch oder finanziell motivierte Angriffe in Deutschland unternommen haben.

APT32	**Alias:** Ocean Lotus
	Zielländer: USA, Myanmar, Thailand, Singapur, Deutschland und China
	Zieltypen: Regierungsbehörden, Unternehmen, aber auch Journalisten, Regimekritiker, Oppositionelle und Menschenrechtler
	2020 soll die Gruppierung u. a. in Deutschland lebende Oppositionelle via Fake-Accounts und Phishing-Webseiten und -Mails ausspioniert haben. Die APT wird als staatlicher Akteur der vietnamesischen Regierung eingestuft. Aktivitäten reichen zurück bis ins Jahr 2014.

[18] Definition APT siehe Seite 45

Wizard Spider	**Alias:** GRIM SPIDER
	Zielländer: Keine präferierten Zielländer
	Zieltypen: Big Game, v.a. Finanz- und Gesundheitswesen
	Wizard Spider verwendet die äußerst prominente Ransomware-Familien Ryuk, welche sehr häufig als nachgeladerte Ransomware-of-Choice einer EMOTET-Infektion eingesetzt wurde.
	Die Gruppierung ist finanziell motiviert, stark und breit vernetzt und gilt als eine der aktivsten Gruppierungen der Cybercrime. Auch in Deutschland kam es 2020 zu Angriffen mit der Ransomware Ryuk.

TA505	**Alias**: FIN11, SectorJ04 Group, GRACEFUL SPIDER, GOLD TAHOE
	Zieltypen: Big Game
	Verwendet "prominente" Malware wie Cl0p, Locky und Dridex und missbraucht kommerzielle Pen-Testing-Tools wie Cobalt Strike. Die Gruppierung zeichnet sich durch ein allgemein hohes Angriffsvolumen aus. TA505 wird für verschiedene schwerwiegende Ransomware-Angriffe in Deutschland verantwortlich gemacht, darunter auf die Symrise AG. Dort kam es durch die Ransomware Cl0p zu einem erheblichen Ausfall der Produktion und Kommunikation. Der dabei entstandene, wirtschaftliche Schaden wird auf mehrere Millionen Euro pro Ausfalltag geschätzt. Eintrittsvektor des Angriffes war ein maliziöses Excel-Dokument, welches bereits Monate vor der Kryptierung des Systems dieses infiltrierte und weitere Schadsoftware nachlud. Mittlerweile konnten die Kernprozesse des Unternehmens wieder hergestellt werden. Auch bei dem Ransomare-Angriff auf die Software AG im Jahr 2020 wird eine Täterschaft von TA505 vermutet.

Abbildung 35: Kurzprofile in Deutschland aktiver Cyber-Akteure

6 Detaillierte Beschreibung herausragender Exekutivmaßnahmen

6.1 DER EMOTET TAKEDOWN

Was ist Emotet?

Erste Identifizierung 2014 - ursprünglich ein Banking-Trojaner. Ab 2017 erfolgte eine Weiterentwicklung der Programmierung des Trojaners hin zu einem sogenannten „Downloader“ (bzw. „Loader“ oder „Dropper“). Primäre Funktion: unbemerkt ein Opfersystem infizieren und weitere Schadsoftware (z. B. Banking-Trojaner „Trickbot“ oder die Ransomware „Ryuk“) nachladen.

Die Nutzung eines durch die Täter geschaffenen Botnetzes zusammen mit der Nachladefunktion von beliebiger Schadsoftware bot weiteren Kriminellen die Grundlage für zielgerichtete Cyber-Angriffe und machte die Malware gerade deshalb innerhalb der Underground Economy so beliebt.

Alleine in Deutschland wurde durch Infektionen mit der Malware Emotet oder durch nachgeladene Schadsoftware ein Schaden in Höhe von mindestens 14,5 Millionen Euro verursacht.[19]

Das Ermittlungsverfahren

Das BKA führt seit September 2018 unter Sachleitung der Generalstaatsanwaltschaft Frankfurt/Main, Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), ein Verfahren gegen die Betreiber von Emotet. Im Rahmen der Ermittlungen konnte die Infrastruktur des Emotet-Botnetzes aufgehellt und ein als Infrastrukturdienstleister fungierender, ukrainischer Staatsangehöriger identifiziert werden.

Der Takedown

Ab dem 26.01.21 wurden in enger Abstimmung mit internationalen Partnerbehörden Exekutivmaßnahmen umgesetzt. Zu unseren Partnern gehörten die Niederlande (NHTCU), Großbritannien (NCA), Frankreich (Nationalpolizei) sowie die USA (FBI). Ein ukrainischer Beschuldigter konnte in seiner Wohnung durch ukrainische Spezialkräfte am offenen Rechner vorläufig festgenommen werden. Durch die forensische Sicherung seiner technischen Geräte konnten die für den Takedown notwendigen Zugangsdaten für die Systeme der Emotet-Infrastruktur erlangt werden.

Auf diese Weise konnte ein zuvor angepasstes „Binary“ erfolgreich an die infizierten Clients des Emotet-Botnetzes verschickt werden, wodurch die Schadsoftware auf den betroffenen Opfersystemen in Quarantäne verschoben wurde. Die infizierten Systeme kommunizierten statt mit dem Täter-Kontrollserver infolgedessen mit einer von den Strafverfolgungsbehörden eingerichteten Infrastruktur, um eine Identifizierung zur Beweissicherung und Benachrichtigung der Opfer über das BSI zu gewährleisten.

[19] Pressemitteilung der GenStA Frankfurt/M. vom 27.01.21

Durch dieses Vorgehen wurde die Schadsoftware Emotet auf den infizierten Systemen unbrauchbar gemacht und den Tätern gleichzeitig jede Möglichkeit genommen, die Kontrolle über ihre Infrastruktur zurückzuerlangen.

Bis April 2021 kommunizierten mehr als 50.000 Bots zum sog. Sinkhole.[20] Das durch die Strafverfolgungsbehörden ausgelieferte Emotet-Binary deinstallierte sich automatisch am 25.04.21, sofern das betroffene System nicht schon zuvor durch den Besitzer bereinigt wurde.

Im Rahmen der Durchsuchungsmaßnahmen in der Ukraine konnten umfangreiche Beweismittel erlangt werden.

Die Folgen

Emotet galt nicht nur als eine der schädlichsten Malware-Varianten, sondern auch als Paradebeispiel für Cybercrime-as-a-Service. Auch wenn einzelne Emotet-Samples weiterhin "in the wild" unterwegs sein werden, so ist die ursprüngliche kriminelle Infrastruktur zerschlagen.

Maßgeblich für diese erfolgreiche Ermittlungsführung war die hervorragende Zusammenarbeit auf nationaler und internationaler Ebene mit (internationalen) Strafverfolgungsbehörden, IT-Sicherheitsbehörden sowie dem Privatsektor.

6.2 DARKNET-MARKTPLATZ „DARKMARKET“

Das Ermittlungsverfahren





Das LKA Rheinland-Pfalz führt seit 2015 unter der Sachleitung der Generalstaatsanwaltschaft Koblenz – ZAC – ein Ermittlungsverfahren gegen die verantwortlichen Betreiber eines Bulletproofhosters, des sogenannten Cyberbunkers in Traben-Trarbach.

Im Rahmen der Ermittlungen[21] wurde festgestellt, dass bis zu diesem Zeitpunkt unbekannte Täter die Infrastruktur des Cyberbunkers nutzten, um auf einer Website mit dem Namen „DarkMarket" im Tor-Netzwerk inkriminierte Güter (Betäubungsmittel, Falschgeld, Kreditkartendaten, etc.) zum Kauf anzubieten. Nach Schließung des Cyberbunkers mussten Anbieter bzw. Kunden auf einen neuen Serverstandort ausweichen.

Der Takedown

Durch umfangreiche, auch internationale, Fahndungs- und Observationsmaßnahmen, konnte der Hauptbeschuldigte in Kooperation mit dänischen Sicherheitskräften im Januar 2021 im Großraum Flensburg festgenommen werden.

[20] Sinkholing bezeichnet eine bestimmte Technik, bei der Informationen von einem ursprünglichen Ziel zu einem anderen Ort umgeleitet werden, der durch den Betreiber des Sinkholes vorgegeben wird.
[21] GStA Koblenz und LKA Rheinland-Pfalz: *https://www.presseportal.de/blaulicht/pm/29763/4566006*

Mit Unterstützung des BKA gelang es der ZKI Oldenburg, einen Großteil der Serverinfrastruktur von „DarkMarket“ in der Ukraine und der Republik Moldau zu lokalisieren.

Der Marktplatz „DarkMarket“, der zuletzt von ca. 500.000 Personen genutzt wurde und auf dem unter anderem digitale Identitäten, Rauschgift, gefälschte Waren, Malware und Hosting-Services angeboten wurden, war seit Juni 2019 aktiv. Als Verkäufer waren ca. 2.400 User registriert.

Insgesamt wurden mindestens 320.000 Geschäfte abgewickelt und dabei mehr als 4.650 Bitcoin und 12.800 Monero bewegt. Dies entspricht anhand des Kurswertes Anfang 2021 mehr als 140 Millionen Euro.

6.3 ALTERNATIVE MARKTPLÄTZE – TELEGRAM-GRUPPEN

Das Ermittlungsverfahren

Das BKA hat im Jahr 2020 gegen mehrere Betreiber illegaler Handelsplattformen auf dem Messenger Telegram ermittelt und neun Gruppen geschlossen.



Die Telegram-Gruppe

Bei dem Handel mit illegalen Waren und Dienstleistungen über Telegram handelt es sich um eine Alternative zu Handelsplattformen im „Darknet“. Dabei erfolgt in den teilweise öffentlich zugänglichen Kanälen und Chatgruppen die Anbahnung der illegalen Geschäfte, etwa durch mit Bildern beworbene Angebote oder durch Listen verifizierter Händler. Die Abwicklung der illegalen Geschäfte zwischen Händler und Käufer erfolgt danach in separaten Chats zwischen einzelnen Telegram-Nutzern.

Der Takedown

Bei einer konzertierten Aktion der Generalstaatsanwaltschaft Frankfurt am Main – ZIT, des BKA und weiteren Strafverfolgungsbehörden am 29.10.20 wurden insgesamt neun Chatgruppen mit ca. 8.000 Mitgliedern im Messenger-Dienst Telegram übernommen und die zugehörigen Daten sichergestellt.

Die bundesweiten Ermittlungen gegen Administratoren entsprechender Gruppen sowie dortige Händler werden seit Anfang Juni 2020 geführt und haben zur Identifizierung von 28 Beschuldigten geführt, gegen die Durchsuchungsbeschlüsse in 30 Objekten vollstreckt werden konnten. Diese Beschuldigten stehen unter anderem im Verdacht, unerlaubt Handel mit Betäubungsmitteln, gefälschten Dokumenten, illegal erlangten Daten und anderen inkriminierten Gütern über Telegram betrieben zu haben.

6.4 DAS ONLINEFORUM „CRIMENETWORK.CO“

Das Ermittlungsverfahren



Seit August 2019 ermittelte die Polizei unter Leitung des Cyber-Competence-Centers des LKA Brandenburg in Form einer länderübergreifenden Ermittlungsgruppe gegen Betreiber des Onlineforum **crimenetwork.co.**

Beteiligt waren die Länderpolizeien Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein sowie das BKA und Europol.

Das Onlineforum

Der nahezu ausschließliche Zweck des Forums lag im Handel und Austausch von Informationen, Werkzeugen und Waren, die entweder direkt aus Straftaten stammen oder der unmittelbaren Begehung weiterer Straftaten dienen. Dabei handelt es sich unter anderem um die Bezahlung von Online-Bestellungen mit fremden Zahlungsdaten oder das Erlangen von betrügerischen Gutschriften von unwissenden Geschädigten. Zudem dient die Plattform als Handelsplatz unter anderem für den Verkauf von Betäubungsmitteln, Hacker-Tools, Botnetzen, Falschgeld, illegal beschaffter Konten- und Kreditkartendaten sowie vornehmlich Hieb- und Stichwaffen.

Operativen Maßnahmen

Etwa 1.500 eingesetzte Polizistinnen und Polizisten nahezu aller Bundesländer mit Unterstützung der Polizei aus Österreich und Polen haben am 22. und 23. Juni 2020 im Rahmen von 328 Ermittlungsverfahren insgesamt 232 Durchsuchungsbeschlüsse vollstreckt.

In diesem Zusammenhang gab es 32 Festnahmen und 9 vollstreckte Haftbefehle. Die Ermittler stellten bei den Durchsuchungen von Wohnungen und Geschäftsräumen sowie anderen Besitztümern zahlreiche Betäubungsmittel (ca. 19 kg Marihuana, ca. 5 kg Amphetamine, sechs Cannabis-Plantagen), 285 Laptops/PC, 461 Mobilfunktelefone/Tablets und andere Datenträger (insgesamt ca. 335 TB Daten), 55.000 Euro Bargeld, Unterlagen von mutmaßlichen Cyberkriminellen und Drogendealern sowie 11 Schusswaffen sicher. Auch die szenetypischen digitalen Währungen (z. B. Bitcoin, Ether) im Wert von ca. 45.000 Euro waren darunter.

Vorangegangen war dem bundesweiten Action-Day die Festnahme des damals 26-jährigen deutschen Administrators des Forums bei der Einreise nach Deutschland im Frühjahr 2019. Um der Entdeckung durch Strafverfolgungsbehörden entgehen zu können, tauschten die Nutzer auf crimenetwork.co gezielt Anleitungen zum Verhalten bei Durchsuchungen, zur Anonymisierung im Internet und Verschlüsselung von Daten. Daher wurde bei 22 Durchsuchungsobjekten der Zugriff mit Spezialeinheiten durchgeführt.

6.5 EV WELLE

Verfahrenshintergrund



Das LKA Schleswig-Holstein führt seit 2019 zusammen mit dem BKA in einer gemeinsamen Ermittlungsgruppe ein Ermittlungsverfahren gegen zwei Beschuldigte u. a. wegen des Verdachts der Computersabotage im besonders schweren Fall.

Beide Personen stehen im Verdacht, DDoS-Angriffe unter anderem gegen mehrere DSL-Provider in Deutschland sowie Unternehmen aus dem Finanzsektor mit einem eigens von ihnen konzipierten und aufgesetzten Botnetz ausgeführt zu haben.

Einer der Täter war maßgeblich für die Anmietung der notwendigen Server-Infrastrukturen verantwortlich, beschaffte Accounts bei externen DDoS-Diensten für nachrangig genutzte Angriffe und führte auch eigene DDoS-Angriffe mit dem Botnetz aus. Ein Angriff gegen ein deutsches Finanzunternehmen war in diesem Zusammenhang sehr öffentlichkeitswirksam, da sich entsprechende Abwehrmaßnahmen anfänglich als nur wenig wirksam erwiesen. Die Webseite des Unternehmens sowie das zugehörige Online-Banking-System waren für die Kunden über mehrere Tage zeitweise nicht erreichbar.

Durch den Ausfall der Systeme bei den unterschiedlichen Geschädigten, durch den Reputationsverlust und durch technische Maßnahmen, die z. T. durch externe Dienstleister unterstützt wurden, ist derzeit von einem Gesamtschaden in Höhe von ca. 5 Millionen Euro auszugehen. Finanzielle Forderungen wurden im Kontext der DDoS-Angriffe nicht gestellt.

Durch die anschließende Auswertung der sichergestellten Server, welche für die DDoS-Angriffe verwendet wurden, konnte festgestellt werden, dass es sich um kompromittierte Server des Online-Spiels „Minecraft“ handelte.

Operative Maßnahmen

Nach ihrer Identifizierung wurden im Juni 2020 die Wohnungen der beiden Beschuldigten durchsucht und umfangreiches Beweismaterial sichergestellt.

Noch vor Durchsuchungsbeginn lief ein wirksamer DDoS-Angriff auf einen Telekommunikationsdienstleister, der sodann beendet werden konnte. Einer der Täter wurde dadurch auf frischer Tat überführt – die notwendigen Tathandlungen waren direkt auf seinem entsperrten Rechner nachvollziehbar.

7 Quo vadis, Cybercrime?

Generell verlagert sich die Kriminalität zunehmend in den digitalen Raum. Im Berichtszeitraum 2020 sind Straftaten unter Nutzung des Tatmittels Internet (Cybercrime im weiteren Sinne) im Vergleich zum Vorjahr um 8,7 % gestiegen. Speziell die Deliktsfelder der Cybercrime im engeren Sinne weisen in den letzten Jahren einen kontinuierlichen Anstieg auf – im Jahr 2020 um 7,9 % verglichen mit dem Jahr 2019.

Die Intensität der verzeichneten Angriffe steigt phänomenübergreifend.

Die Feststellungen und Fallbeispiele des Bundeslagebildes 2020 zeigen allerdings auch in qualitativer Hinsicht eine weitere Steigerung im Tätervorgehen.

Die zunehmende Professionalisierung der Täterseite hat die Cybercrime-Bedrohungslage in Deutschland weiter verschärft – die Modi Operandi werden komplexer und ihr jeweiliges Zusammenspiel sowie die Art der verwendeten Angriffsvektoren ausgefeilter und vielfältiger. Das zunehmend professionalisierte Vorgehen von auch allgemein-kriminell motivierten Gruppierungen bzw. Tätern übernimmt APT-artige Vorgehensweisen und verschärft die Bedrohungslage zusätzlich.

Die zunehmende Digitalisierung in allen Lebensbereichen schafft mehr Tatgelegenheiten, während das Phänomen des „Cybercrime-as-a-Service" die Eintrittsschranken bei der Begehung von Straftaten im Cyber-Bereich weiter absenkt. Darüber hinaus steigt mit jedem erfolgreichen Angriff das kriminelle Potenzial der Underground Economy und damit ihre Möglichkeiten, neue Malware zu entwickeln und komplexe Angriffe durchzuführen.

Cybercrime – ein hochkomplexer, krimineller Wirtschaftszweig mit eigenen Wertschöpfungsketten.

Neben dem „Faktor Mensch" sind vor allem unsichere IT-Systeme ein beliebtes Einfallstor. Unzureichend gesicherte oder falsch konfigurierte Datenbanken, kritische Schwachstellen in Remote-Zugängen oder fehlende Sicherheitsprogramme und Schutzmaßnahmen für gewerbliche oder private IT-Infrastrukturen ermöglichen es Angreifern, in ein Zielsystem einzudringen und es zu kompromittieren.

Auch laut Risiko-Barometer 2021 der Allianz Global Corporate & Specialty gehören mangelnde Sicherheitsvorkehrungen und Data-Breaches zu den größten Risiken für Unternehmen.[22] Die Verteilung von Ransomware sowie auch DDoS-Angriffe, gekoppelt mit erpresserischen Forderungen, werden nicht nur die Strafverfolgungsbehörden künftig weiter erheblich beschäftigen.

Kritische Infrastrukturen, öffentliche Verwaltungen und die deutsche Wirtschaft hängen in hohem Maße von einer funktionierenden, verlässlichen IT-Infrastruktur ab.

Cyber-Angriffe können in der eng verzahnten, globalisierten Welt mit komplexen Prozessabläufen und Lieferverbindungen enorme Dominoeffekte erzeugen, die massive Schäden mit sich bringen.

Laut Studie der Initiative „Deutschland sicher im Netz" sind mehr als die Hälfte der Unternehmen in ihrer Existenz gefährdet, wenn sensible Daten im Zuge eines Cyberangriffes verloren gehen. Ebenfalls gaben 46 % der befragten Unternehmen an, bereits einmal oder mehrere Male Opfer eines Cyberangriffs geworden zu sein. [23]

---

[22] Das Allianz-Risikobarometer kann hier abgerufen werden: *https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021-de.html*

[23] Der Praxisreport 2020 Mittelstand @IT-Sicherheit der Initiative „Deutschland sicher im Netz" ist hier abrufbar: *https://www.sicher-im-netz.de/dsin-praxisreport-2020-mittelstand-it-sicherheit*

Diese und weitere Studien weisen darauf hin, dass die Dunkelziffer im Cyber-Bereich weiterhin hoch ist: Wie ein in 2020 veröffentlichter Forschungsbericht des Bundesministeriums für Wirtschaft und Energie (BMWi) ausführt, waren etwa zwei Drittel der im Zeitraum 2018-2019 befragten Unternehmen (65 %) bereits von mindestens einem Cyber-Angriff betroffen, von denen lediglich 11,9 % Anzeige erstatten. [24]

Ransomware- und DDoS-Angriffe – eine existentielle Bedrohung für die Wirtschaft.

Dabei ist die Bedrohungslage besonders für Unternehmen sehr hoch: Die Wahrscheinlichkeit, Opfer eines Ransomware-Angriffes zu werden, korreliert mit der Größe des Unternehmens. Während nur etwa jedes neunte kleine Unternehmen Opfer eines Ransomware-Angriffs wurde, betraf es jedes vierte bis fünfte große Unternehmen ab 500 Beschäftigten.

Eintrittsvektor für Cyberattacken ist nicht immer das Unternehmen selbst – oftmals nutzen Cyberkriminelle die Lieferkette des Unternehmens oder die IT-Systeme des Partners oder IT-Dienstleisters aus, um das eigentliche Ziel zu kompromittieren.

Aufgrund der anhaltenden, globalen Corona-Pandemie werden auch weiterhin vermehrt das Internet bzw. digitale Dienste – z. B. für Homeoffice und Home-Schooling – genutzt. Für 2021 bedeutet dies breit gefächerte Angriffspotenziale für Cyber-Kriminelle.

Die Corona-Pandemie zeigt den opportunistischen Charakter von Cyber-Kriminellen: Es werden jene angegriffen, welche für die Gesellschaft einen hohen Stellenwert besitzen.

Der erfolgreiche Abschluss der Impfkampagne stellt einen wichtigen Meilenstein bei der Überwindung der Corona-Pandemie dar. Neben seiner primären Funktion als Vakzin liegt dem Impfstoff demzufolge auch ein hoher symbolhafter, sozialer, politischer und ökonomischer Wert zugrunde. Mit der Erforschung, Herstellung und Distribution des Corona-Impfstoffs steigt die gesellschaftliche, politische, aber auch wirtschaftliche Bedeutung ganzer Industriezweige – die folglich auch für Täter im Bereich der Cybercrime im Jahr 2021 immer interessanter werden.

In allen betreffenden Bereichen werden sich absehbar weitere Angriffsziele für Cybertäter auftun. In der Gesamtschau kann somit prognostiziert werden, dass Cybercrime auch in 2021 weiter an Relevanz gewinnen wird.

[24] Forschungsprojekt der IT-Sicherheitsinitiative des BMWi: „Cyberangriffe gegen Unternehmen in Deutschland“ – siehe hier: *https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Publikationen/cyberangriffe-gegen-unternehmen-in-deutschland.html*



Abbildung 36: Ausblick – Cybercrime 2021

8 Appendix

8.1 STRAFTATBESTÄNDE CCIES



Nachfolgend werden die relevanten Straftatbestände von Cybercrime im engeren Sinne beschrieben.

Computerbetrug als Cybercrime im engeren Sinne (§ 263a StGB)

Dieses Delikt wird seit 01.01.2016 in der PKS in folgende Betrugsarten aufgeschlüsselt:

- Betrügerisches Erlangen von Kraftfahrzeugen gem. § 263a StGB,
- weitere Arten des Kreditbetruges gem. § 263a StGB,
- Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB,
- Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB,
- Leistungskreditbetrug gem. § 263a StGB,
- Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB,
- Überweisungsbetrug gem. § 263a StGB.

Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB)

Dies stellt eine besondere, separat erfasste Form des Computerbetrugs gem. § 263a StGB dar. Unter Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen werden sowohl bei Firmen als auch Privathaushalten, z. B. durch den unberechtigten Zugriff auf Router, teure Auslandstelefonverbindungen angewählt oder gezielt Premium- bzw. Mehrwertdienste in Anspruch genommen.

Sonstiger Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB)

Soweit nicht unter die erstgenannten Betrugsarten bzw. die „Missbräuchliche Nutzung von Telekommunikationsdiensten“ gefasst.

Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Daten-Hehlerei (§§ 202a, 202b, 202c, 202d StGB)

Umfasst den Diebstahl und die Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden i. d. R. als Handelsware auf digitalen Schwarzmärkten zum Kauf angeboten und täterseitig missbräuchlich eingesetzt.
Die Verwertung erfolgt damit in zwei Stufen:

1. dem Verkauf der Daten
2. dem betrügerischen Einsatz der erworbenen Daten

Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB)

Diese Tatbestände beinhalten die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z. B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen.

Unter Vortäuschung einer Legende soll der Geschädigte z. B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

Datenveränderung/Computersabotage (§§ 303a, 303b StGB)

Hierbei handelt es sich um eine Art digitaler Sachbeschädigung. Es wird die Veränderung von Daten in einem Datenverarbeitungssystem bzw. das Verändern des Systems durch andere als den Dateninhaber unter Strafe gestellt.

Die §§ 303a, 303b StGB umfassen typischerweise Denial of Service-Angriffe (DoS-/DDoS-Angriffe), ebenso wie die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojaner, Viren, Würmer usw.).

8.2 WICHTIGE DEFINITIONEN / GLOSSAR

Definition „Cybercrime im engeren Sinne“



Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten

Definition „Cybercrime im weiteren Sinne“



Straftaten, die unter Nutzung von Informationstechnik begangen werden (Tatmittel Internet)

Definition „Underground Economy“

Die Gesamtheit aller täterseitig illegal genutzten Plattformen. Sie stellen eine kommerziell ausgerichtete, dynamische Landschaft dar, welche Kommunikations- und Verkaufsplattformen im Internet vereint.

Aufgrund der starken wirtschaftlichen und illegalen Ausrichtung der Plattformen werden sie unter dem Begriff „Underground Economy“ zusammengefasst.

Clearnet *(Visible Web, Surface Web, Open Web)*



Für jedermann mit marktgängigen Browserprogrammen zugänglich, unterstützt durch einfache Handhabung mittels Suchmaschinen.

Auch im Clearnet sind vielfältige illegale Inhalte verfügbar, z. B. solche mit Bezug zu Politisch Motivierter Kriminalität oder Plattformen und Foren der sog. „Underground Economy“ (Straftaten überwiegend aus dem Bereich der Cybercrime im engeren Sinne).

Deep Web *(Invisible Web)*

Der Teil des Internets, dessen Inhalte nicht durch Suchmaschinen auffindbar sind, weil z. B. Webseiten nicht indexiert/in Suchmaschinen verlinkt wurden oder weil sie zugriffsbeschränkt sind. Inhalte des Deep Webs können z. B. Datenbanken, Intranets oder Fachwebseiten sein und sind – sofern die URL bekannt ist und eine Zugangsberechtigung besteht – mit Browsern erreichbar.

Darknet



Darknet-Inhalte sind ausschließlich durch Nutzung spezieller Software, die der Anonymisierung dient, einsehbar.

Bestandteile des Darknets sind z. B. Foren, Blogs/Wikis mit unterschiedlichsten – legalen wie illegalen – Zielrichtungen. Einen bedeutenden Teil machen sog. Darknet-Marktplätze aus, bei denen größtenteils inkriminierte Güter gehandelt werden. Auch werden zahlreiche und bedarfsorientierte Angebote für Cybercrime-as-a-Service (Durchführung bzw. Unterstützungsleistungen krimineller Handlungen im Auftrag) oder Darknet-Seiten mit kinderpornografischen Inhalten zur Verfügung gestellt.

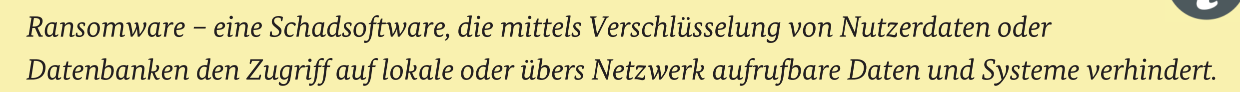
Was ist Malware?



Unter dem Begriff Malware versteht man alle Programme, welche schädliche Funktionen auf einem IT-System ausführen. Zu diesen maliziösen Funktionen gehören u. a.

- *Ausspähen und Weiterleiten von Account-Daten wie Usernamen und Passwörtern,*
- *Manipulation bzw. Zerstörung von Daten,*
- *illegitime Nutzung von Rechenleistung zum Kryptomining,*
- *Verschlüsseln von Daten,*
- *Einbindung in ein Bot-Netz und zum Missbrauch für DDoS-Angriffe,*
- *missbräuchliche Fernsteuerung eines fremden IT-Systems.*

Was ist „Ransomware"?



Ransomware – eine Schadsoftware, die mittels Verschlüsselung von Nutzerdaten oder Datenbanken den Zugriff auf lokale oder übers Netzwerk aufrufbare Daten und Systeme verhindert.

Wird man Opfer eines solchen Angriffs erfolgt i. d. R. eine Lösegeldforderung (Ransom) – in digitaler Währung – seitens der Täter, die erst nach Eingang der geforderten Lösegeldsumme die Verschlüsselung aufheben. Um den Druck auf die Opfer zu erhöhen, werden zudem kurze Fristen gesetzt. Zudem wird mit der Löschung oder Veröffentlichung von Daten gedroht, wenn der Aufforderung nicht rechtzeitig nachgekommen wird.

Definition „Ransomware-as-a-Service"

Ransomware, die in Form einer „Dienstleistung" betrieben wird, stellt eine besondere Form der Ransomware dar – die sogenannte „Ransomware-as-a-Sercive".

Distributed Denial of Service (DDoS)-Angriffe



Durch gezielt herbeigeführte Überlastung wird versucht, die Verfügbarkeit eines Internetdienstes oder eines Zielsystems zu stören.

Der DDoS-Angriff zeichnet sich dadurch aus, dass der Angriff i. d. R. von einer Vielzahl einzelner Anfragen bzw. einer großen Zahl an Rechnern – vielfach mittels großer, ferngesteuerter Botnetze – erfolgt.

Botnetze



Botnetze entstehen durch die zumeist unbemerkte Installation einer Schadsoftware auf PCs von Geschädigten. Die infizierten Geräte werden dann ohne Wissen ihrer Besitzer mittels sog. „Command & Control-Server" kontrolliert, gesteuert und zu einem Botnetz zusammengeschaltet, sodass Massenabfragen erfolgen können.

Advanced Persistant Threats (APT)



Bei einem APT handelt es sich um einen zielgerichteten Cyber-Angriff auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind i. d. R. schwierig zu detektieren.

APT sind dabei nicht ausschließlich staatliche Akteure: Die ENISA (European Union Agency for Cybersecurity) stellte fest[25], dass nur 16 % der dort identifizierten Akteure staatlich motiviert sind – 60 % lassen sich der organisierten Kriminalität zuordnen.[26]

8.3 DIE NEUN SÄULEN DER CYBERCRIME

Der Phänomenbereich der Cybercrime im engeren Sinne (CCieS) wird durch eine hohe Arbeitsteilung zwischen Tatbeteiligten sowie der für die Begehung der Gesamttat notwendigen Tatkomponenten geprägt. Nur noch wenige Cyberkriminelle können heutzutage ihre Taten alleine und ohne wesentliche Unterstützungshandlungen Dritter begehen. Daher kommt es zu einer stetig voranschreitenden Spezialisierung einzelner Cybercrime-as-a-Service-Anbieter. Das wiederum ermöglicht auch technisch weniger versierten Tätern komplexere Straftaten zu begehen. Folglich können die entsprechenden Akteure alle technisch komplexen Tatbeiträge zunehmend outsourcen und dafür kompetente Dienstleister einkaufen. Hierbei konnten, nach aktuellem Ermittlungsstand des BKA, neun essentielle Säulen identifiziert werden:

[25] ENISA Threat Landscape 2020 - Main Incidents; online abrufbar unter: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents*

[26] Hinweis: Akteure aus der Cybercrime, v.a. staatliche Akteure, werden häufig mit dem Kürzel APT, gefolgt von einer fortlaufenden Nummerierung benannt. Diese Namensgebung ist allerdings nicht einheitlich definiert. Andere Namenskonventionen umfassen die Nutzung des Kürzels TA (für Threat Actor – gefolgt von einer Nummer) oder der Verwendung von Tieren als Teil eines eindeutigen Namens wie KRYPTONITE PANDA, STATIC KITTEN oder WIZARD SPIDER. Jedes Tier steht hier für die Herkunft oder Art des Akteurs (PANDA für Akteure aus China, Kitten aus dem Iran und Spider v.a. für finanziell motivierte Gruppierungen).



Säule 1

Foren und Jabber-Server
Repräsentieren digitale Plätze zum Austausch von Kontakten und Diensteanbietern und fungieren somit als „Gelbe Seiten“ für Cyberkriminelle. Hierdurch finden Anbieter und Bedarfsträger zusammen.
Es handelt sich um das „Eintrittstor“ in die Underground Economy.



Säule 2

Bulletproofhosting & Proxyprovider
Auf Täterseite werden zur Tatbegehung oftmals inkriminierte, „robuste“ Infrastrukturen benötigt; die selbst bei missbräuchlicher Nutzung eine längere Zeit online bleiben und nicht direkt durch den Provider abgeschaltet werden können. Für derartige Dienstleistungen werden spezielle inkriminierte Provider genutzt. Außerdem gehören Proxy- bzw. VPN-Provider zur Basisausstattung und verschleiern die IP-Adressen der kriminellen Nutzer.



Säule 3

Marktplätze, Shops und Automated Vending Carts (AVC)
Für viele Cyberstraftaten benötigen Täter kompromittierte Zugangsdaten. Diese erhalten sie über zentralisierte und weitestgehend automatisierte Vertriebsplattformen sog. Marktplätze. Diese stellen einen großen Anteil strafrechtlich relevanter Inhalte im Darknet dar. Sie sind ähnlich aufgebaut wie kommerzielle E-Commerce Plattformen (Amazon, ebay etc.).



Säule 4

Malwareentwicklung & Coding
Die bedarfsorientierte Entwicklung von Schadsoftware richtet sich nach den spezifischen Anforderungen des Bedarfsträgers und dem Entwicklungsaufwand. Zudem spielen auch die Preisvorstellungen des Auftraggebers eine Rolle. Simple Malware ist bereits für 5.000 Euro erhältlich.



Säule 5

Malware Crypting & Obfuscation
Crypting beschreibt den Prozess des Überarbeitens und Verschlüsselns des maliziösen Codes, welcher nicht mehr durch den Entwickler selbst, sondern durch einen sog. „Crypter“, also einen spezialisierten Dienstleister, vorgenommen wird. Dieses Abhärten bzw. Verbessern einer Malware dient oftmals der Steigerung der Malware-Tarnfähigkeit (sog. Obfuskation).



Säule 6

Counter-Antivirus-Services (CAV)
Beschreibt den Service der Malware-Prüfung, um festzustellen, ob diese durch gängige Anti-Viren-Programme erkannt werden könnte.
Der Service kann je nach Bedarf "abonniert" werden und dem Kunden z. B. täglich Auskunft über die Effektivität der verwendeten Malware und deren Verschleierung geben.



Säule 7

Malware Delivery & Infection on Demand & PPI
Das Ausrollen und Installieren der Schadsoftware stellt einen weiteren wichtigen Schritt in der Verwertungskette dar. Die Kosten der Distribution orientieren sich an der Art der zu verbreitenden Malware sowie der Dauer der in Anspruch genommenen Leistung: Die Streuung der Malware erfolgt z. B. via Malspam, Phishing oder Drive-By-Infection.



Säule 8

Drops, Mules & Cashout
Inkriminierte Zahlungen müssen auf Konten geleitet und an Geldautomaten in bar abgehoben werden.
Diese achte Säule fasst die aus Tätersicht mit Abstand risikoreichsten Aktivitäten zusammen, da hier in aller Regel ein Erscheinen des Täters oder der durch ihn beauftragen Läufer (sog. Runner/Drops) in der realen Welt erforderlich ist. Die Entgelte orientieren sich i. d. R. prozentual an den Umsätzen / dem Wert der Transaktion.



Säule 9

Exchanger – Die digitale Geldwäsche
Die „Exchanger“ bestreiten die „letzte Meile“ zum (kriminellen) Kunden und sorgen dafür, dass die beim Cyberkriminellen in einer Währung seiner Wahl eingegangenen Finanzmittel keiner konkreten Straftat mehr zugeordnet werden können.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
April 2021

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

Weitere Lagebilder des Bundeskriminalamtes zum Herunterladen finden Sie ebenfalls unter:
www.bka.de/Lagebilder

Diese Publikation wird vom Bundeskriminalamt im Rahmen der Öffentlichkeitsarbeit herausgegeben.
Die Publikation wird kostenlos zur Verfügung gestellt und ist nicht zum Verkauf bestimmt.